CORE
Metadata, citation and similar papers at core.ac.uk
Provided by Elsevier - Publisher Connector

ELSEVIER
Journal of Pure and Applied Algebra 160 (2001) 123–156
JOURNAL OF PURE AND APPLIED ALGEBRA
www.elsevier.com/locate/jpaa

The geometry monoid of left self-distributivity

Patrick Dehornoy
Laboratoire SDAD, ESA 6081 CNRS, Mathématiques, BP 5186, Université Campus II, 14032 Caen, France

Received 9 July 1999; received in revised form 10 February 2000
Communicated by A. Blass

Abstract

We develop a counterpart to Garside's analysis of the braid monoid B_n^+ relevant for the monoid M_{LD} that describes the geometry of the left self-distributivity identity. The monoid M_{LD} extends B_∞^+, of which it shares many properties, with the exception that it is not a direct limit of finitely generated monoids. By introducing a convenient local version of the fundamental elements Δ, we prove that right least common multiples exist in M_{LD}, and, more generally, that M_{LD} resembles a generalized Artin monoid. © 2001 Elsevier Science B.V. All rights reserved.

MSC: 20F36; 20N02

0. Introduction

Applying a given algebraic identity (I) to a formal expression can be seen as defining an action of a certain monoid $\mathscr{G}_I$ associated with (I). In the case of the associativity identity, the involved monoid happens to be a group, namely Thompson's group F of [16], a remarkable group which appears in several independent domains [13]. Here, we consider the case of the left self-distributivity identity

$$x(yz) = (xy)(xz), \qquad (LD).$$

E-mail address: dehornoy@math.unicaen.fr (P. Dehornoy).

0022-4049/01/\$ - see front matter © 2001 Elsevier Science B.V. All rights reserved.
PII: S0022-4049(00)00081-5

This identity has been widely investigated in the recent years due to its deep connection with properties of large cardinals in set theory [14,15] and with Artin's braid groups. In particular, the connection with braids originates in the fact that, in the case of Identity (LD), the monoid $\mathcal{G}_{LD}$ alluded to above turns out to be closely related with some group G_{LD} that is an extension of Artin's braid group B_∞. The group G_{LD}, which appears as a natural counterpart to Thompson's group F when left self-distributivity replaces associativity, is an interesting object in itself. It has already been investigated in [2,4], leading to new results about Artin's braid groups B_n such as the existence of a left invariant linear ordering and a new efficient solution to the word problem. The aim of the current paper is to continue the study of this group.

Keeping in mind that the braid group B_∞ is a projection of the group G_{LD}, we show how to develop a counterpart to Garside's analysis of the braid groups for G_{LD}. In particular, starting with a monoid presentation of G_{LD}, we consider the associated monoid M_{LD} and investigate the connection between G_{LD} and fractions from M_{LD}. Technically, things are more complicated than in the case of braids because, in contradistinction to B_∞, which is the direct limit of the groups B_n, the group G_{LD} has no natural approximations by finite type groups. Thus, we cannot resort to Garside's fundamental elements Δ_n. The aim of this paper is to show how to overcome the problem by considering a sort of local version Δ_t of the elements Δ_n and analysing the simple elements of M_{LD} defined as those elements that divide some Δ_t. In this approach, using the action of $\mathcal{G}_{LD}$ *via* self-distributivity provides one with useful intuitions. In particular, we obtain with the equivalence of two natural notions of simple elements a convenient infinitary version of the well-known exchange lemma for Coxeter groups, and we hope that the methods we introduce here can be applied to further infinitary Artin-like groups in the future.

The main results we prove here are that right least common multiples exist in the monoid M_{LD}, and that every element of the group G_{LD} can be expressed as a fraction. We also construct in M_{LD} a unique normal form which is reminiscent of the greedy normal form of braids [1,9–11]. It can be noted that, using a projection, we deduce from these results new proofs for their braid counterparts, which can therefore be seen as results about self-distributivity.

It is known that the group G_{LD} faithfully describes the geometry of LD-equivalence in the sense that no other relation than those holding in G_{LD} connects the operators of $\mathcal{G}_{LD}$; on the other hand, whether M_{LD} faithfully describes the geometry of positive LD-equivalence ('LD-expansions') is not known: this actually is equivalent to M_{LD} embedding in G_{LD}. Should this be true, then some algebraic results about M_{LD} like the existence of common right multiples would directly follow from the known properties of LD-expansions, making some computations of this paper unnecessary. Now, the previous embedding result remains out of reach for the moment, and we rather think that a possible proof will come from a better understanding of M_{LD}.

The organization of the paper is as follows. In order to make it self-contained, we recall in Section 1 those definitions and results of [2,4] that are used in the sequel. In Section 2, we establish the confluence property in M_{LD}, i.e., the existence of right common multiples, by syntactically imitating the proof of the confluence property for left self-distributivity [2]. In Section 3, we introduce simple elements of M_{LD}, and prove the equivalence of a syntactic and a dynamic characterization of such elements. Finally, we construct in Section 4 a unique normal form for the elements M_{LD}, and briefly discuss the conjecture that M_{LD} embeds in G_{LD}.

1. The geometry monoid of left self-distributivity

1.1. Left self-distributivity operators

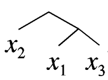
We fix an infinite sequence of variables $x_1, x_2, \ldots$, and let T_∞ be an absolutely free system based on $\{x_1, x_2, \ldots\}$: we can describe T_∞ as the set of all well formed abstract terms constructed using the variables x_i and a binary operation symbol. Thus, x_1 and $x_2 \cdot (x_1 \cdot x_3)$ are typical elements of T_∞. We use T_1 for the set of those terms involving the variable x_1 only. Then T_1 is an absolutely free system based on x_1.

Let us say that two terms t, t' in T_∞ are *LD-equivalent*, denoted $t =_{LD} t'$, if we can transform t to t' by repeatedly applying Identity (LD). In other words, the relation $=_{LD}$ is the congruence on T_∞ generated by all pairs of the form

$$(t_1 \cdot (t_2 \cdot t_3), (t_1 \cdot t_2) \cdot (t_1 \cdot t_3)).$$

Then, by standard arguments, the quotient structure $T_\infty / =_{LD}$ is a free LD-system based on $\{x_1, x_2, \ldots\}$.

The idea is now to describe the LD-equivalence class of a given term t in T_∞ as the orbit of t relatively to the action of some monoid associated with Identity (LD). In order to specify this action precisely, it is convenient to associate with every term in T_∞ a finite binary tree whose leaves are labeled with variables: if t is the variable x, the tree associated with t consists of a single node labeled x, while, for $t = t_1 \cdot t_2$, the binary tree associated with t has a root with two immediate successors, namely a left one which is (the tree associated with) t_1, and a right one which is (the tree associated with) t_2. For instance, the tree associated with the term $x_2 \cdot (x_1 \cdot x_3)$ is



.

We use finite sequences of 0's and 1's as addresses for the nodes in such trees, starting with an empty address ϕ for the root, and using 0 and 1 for going to the left and to the right respectively. For t a term, we define the *outline* of t to be the collection of all addresses of leaves in (the tree associated with) t, and the *skeleton* of t to be the collection of the addresses of nodes in t: thus, for instance, the outline of the term $x_2 \cdot (x_1 \cdot x_3)$ is the set $\{0, 10, 11\}$, while its skeleton is $\{0, 10, 11, 1, \phi\}$, as t comprises three leaves and two inner nodes. For t a term, and α an address in the skeleton of t, we have the natural notion of the αth subterm of t, denoted $\mathrm{sub}(t, \alpha)$: this is the term corresponding to the subtree of the tree associated with t whose root lies at address α. This amounts to defining inductively

$$\mathrm{sub}(t,\alpha) = \begin{cases} t & \text{if } t \text{ is a variable or } \alpha = \phi \text{ holds,} \\ \mathrm{sub}(t_0,\beta) & \text{for } t = t_0 \cdot t_1 \text{ and } \alpha = 0\beta, \\ \mathrm{sub}(t_1,\beta) & \text{for } t = t_0 \cdot t_1 \text{ and } \alpha = 1\beta. \end{cases}$$

Finally, we define the right height $ht_R(t)$ of a term t to be the length of the rightmost branch in the tree associated with t; equivalently, $ht_R(t)$ is the integer inductively defined by $ht_R(t) = 0$ if t is a variable, and $ht_R(t) = ht_R(t_1) + 1$ for $t = t_0 \cdot t_1$.

With the previous notations at hand, we can define the notion of a basic LD-expansion of a term precisely.

Definition. Assume that t is a term, and α is an address such that $\alpha 10$ belongs to the skeleton of t. Then we denote by $(t)\alpha$ the term obtained from by replacing the subterm $\mathrm{sub}(t,\alpha)$ with the term $(\mathrm{sub}(t,\alpha 0) \cdot \mathrm{sub}(t,\alpha 10)) \cdot (\mathrm{sub}(t,\alpha 0) \cdot \mathrm{sub}(t,\alpha 11))$.

Thus $(t)\alpha$ is the term obtained from t by applying left self-distributivity *at* α in the direction $x(yz) \mapsto (xy)(xz)$. The reader can check for instance that, if t is the term $x_1 \cdot x_2 \cdot x_3 \cdot x_4$ — here, and everywhere in the sequel, we take the convention that missing parentheses are to be added on the right, so, for instance, the previous expression stands for $x_1 \cdot (x_2 \cdot (x_3 \cdot x_4))$ — then the only addresses α for which $(t)\alpha$ exists are ϕ and 1, and we have

$$(t)\phi = (x_1 \cdot x_2) \cdot (x_1 \cdot x_3 \cdot x_4) \quad \text{and} \quad (t)1 = x_1 \cdot (x_2 \cdot x_3) \cdot (x_2 \cdot x_4).$$

Definition. We say that the term t' is a *basic LD-expansion* of the term t if we have $t' = (t)\alpha$ for some α; we say that t' is an *LD-expansion* of t if there exists a finite sequence of addresses $\alpha_1, \ldots, \alpha_p$ (possibly $p = 0$) such that t' is $(\ldots((t)\alpha_1)\alpha_2 \ldots)\alpha_p$.

Let $\boldsymbol{A}$ denote the set of all binary addresses, and $\boldsymbol{A}^*$ denote the free monoid of all words on $\boldsymbol{A}$, i.e., of all finite sequences of addresses. For w in $\boldsymbol{A}^*$, say $w = \alpha_1 \cdot \ldots \cdot \alpha_p$, and t a term, we write $(t)w$ for the LD-expansion $(\ldots((t)\alpha_1)\alpha_2 \ldots)\alpha_p$, when it exists. We thus have obtained a partial action (on the right) of the monoid $\boldsymbol{A}^*$ on the set T_∞.

Definition. For every word w in $\boldsymbol{A}^*$, we define LD_w to be the partial operator on T_∞ that maps every sufficiently large term t to its LD-expansion $(t)w$. The monoid consisting of all operators LD_w equipped with reverse composition is denoted by $\mathscr{G}_{LD}^+$.

The following equivalence follows from the definition directly:

Lemma 1.1. *Assume that t, t' are terms in T_∞. Then the following are equivalent*:
(i) *The term t' is an LD-expansion of the term t*;
(ii) *Some element of $\mathscr{G}_{LD}^+$ maps t to t'.*

By construction, if t' is an LD-expansion of t, then t' is LD-equivalent to t. The converse is not true in general, but we can easily describe LD-equivalence by means of an action at the expense of introducing symmetrized operators LD_w^{-1} which correspond to using (LD) in the contracting direction $(xy)(xz) \mapsto x(yz)$. So, for every address α, we introduce LD_α^{-1} to the inverse operator of LD_α (which is injective), and we consider the monoid $\mathscr{G}_{LD}$ generated by all operators LD_α and LD_α^{-1} using reversed composition. By construction, every element in $\mathscr{G}_{LD}$ is a finite product of operators LD_α and LD_α^{-1}. Using $\boldsymbol{A}^{-1}$ for the set consisting of a copy α^{-1} for each address α, and defining $LD_{\alpha^{-1}}$ to be LD_α^{-1}, we can represent every element of $\mathscr{G}_{LD}$ as LD_w, where w is a word on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$, i.e., a finite sequence of signed addresses. We write $(\boldsymbol{A} \cup \boldsymbol{A}^{-1})^*$ for the set of all such words, of which $\phi \cdot 11^{-1} \cdot 0$ is a typical element. We have the following straightforward characterization analogous to Lemma 1.1:

Lemma 1.2. *Assume that t, t' are terms in T_∞. Then the following are equivalent*:
(i) *The terms t and t' are LD-equivalent.*
(ii) *Some element of $\mathscr{G}_{LD}$ maps t to t'.*

The action of the monoid $\mathscr{G}_{LD}$ is a partial action: for w in $(\boldsymbol{A} \cup \boldsymbol{A}^{-1})^*$, the term $(t)w$ need not be defined for every term t, i.e., the domain of the operator LD_w is not the whole of T_∞. In particular, it should be observed that the operator LD_w may be empty: this happens for instance for $w = \phi \cdot 1 \cdot \phi^{-1}$, as no term in the image of $LD_{\phi \cdot 1}$ may belong to the image of LD_ϕ, i.e., to the domain of LD_ϕ^{-1}. However, using the technique of term unification, we can prove the result below. Here, a term is said to be canonical if the list of all variables that occur in t, enumerated from left to right ignoring repetitions, is an initial segment of $(x_1, x_2, \ldots)$. A substitution is defined to be a mapping of $\{x_1, x_2, \ldots\}$ into T_∞, and, if h is a subtitution and t is a term in T_∞, t^h denotes the term obtained from t by replacing each variable x_i with the corresponding term $h(x_i)$. Finally, we say that a term t is injective if every variable occurs at most once in t.

Proposition 1.3. (i) *Assume that w is a word in $(\boldsymbol{A} \cup \boldsymbol{A}^{-1})^*$. Then either the operator LD_w is empty, or there exists a unique pair of LD-equivalent canonical terms $(t_w^{\mathrm{L}}, t_w^{\mathrm{R}})$ such that LD_w maps the term t to the term t' if there exists a substitution h satisfying $t = (t_w^{\mathrm{L}})^h$ and $t' = (t_w^{\mathrm{R}})^h$.*

(ii) *If u is a positive word in $\boldsymbol{A}^*$, then LD_u is nonempty, and the term t_u^{L} is injective; in this case, a term t lies in the domain of the operator LD_u if its skeleton includes the skeleton of t_u^{L}.*

We skip the proof here. It builds on the techniques developed in [2,3] and on the classical method of term unification.

1.2. LD-relations

By definition, the monoid $\mathscr{G}_{LD}^+$ is generated by the family of all operators LD_α, $\alpha \in \boldsymbol{A}$, while the monoid $\mathscr{G}_{LD}$ is generated by the family of all LD_α, $\alpha \in \boldsymbol{A} \cup \boldsymbol{A}^{-1}$.

These monoids are not free: some relations connect the operators LD_α. These relations capture what can be called the geometry of Identity (LD). We say that the address α is a prefix of the address β if β is $\alpha\beta'$ for some β'; we say that two addresses α, β are orthogonal, denoted $\alpha\perp\beta$, if there exists an address γ such that $\gamma0$ is a prefix of α and $\gamma1$ is a prefix of β, or vice versa.

Proposition 1.4 (Dehornoy [2]). *For all α, β in $\boldsymbol{A}$, the following relations hold in the monoid $\mathscr{G}_{LD}$*:

$$LD_\alpha \bullet LD_\beta = LD_\beta \bullet LD_\alpha \quad \text{for } \alpha\perp\beta \quad (\text{type } \perp),$$

$$LD_{\alpha0\beta} \bullet LD_\alpha = LD_\alpha \bullet LD_{\alpha10\beta} \bullet LD_{\alpha00\beta} \quad (\text{type } 0),$$

$$LD_{\alpha10\beta} \bullet LD_\alpha = LD_\alpha \bullet LD_{\alpha01\beta} \quad (\text{type } 10),$$

$$LD_{\alpha11\beta} \bullet LD_\alpha = LD_\alpha \bullet LD_{\alpha11\beta} \quad (\text{type } 11),$$

$$LD_{\alpha1} \bullet LD_\alpha \bullet LD_{\alpha1} \bullet LD_{\alpha0} = LD_\alpha \bullet LD_{\alpha1} \bullet LD_\alpha \quad (\text{type } 1).$$

A direct verification of these equalities is easy. It is less easy to prove that, conversely, the above equalities, together with the fact that LD_α is an inverse of LD_α^{-1}, exhaust the possible relations in $\mathscr{G}_{LD}$, i.e., they constitute a presentation of this monoid. The result is not readily true, as the product of LD_α and LD_α^{-1} is only the identity mapping of its domain, and it is not the identity mapping of T_∞. This seemingly superficial problem cannot be solved, since, as was said above, the product of two elements in $\mathscr{G}_{LD}$ may be empty. However, we have the following result:

Definition. Define an *LD-relation* to be a pair of words on $\boldsymbol{A}$ of one of the following types:

- type ($\perp$): $(\alpha\cdot\beta, \beta\cdot\alpha)$, with $\alpha\perp\beta$;
- type (0): $(\alpha0\beta\cdot\alpha, \alpha\cdot\alpha10\beta\cdot\alpha00\beta)$;
- type (10): $(\alpha10\beta\cdot\alpha, \alpha\cdot\alpha01\beta)$;
- type (11): $(\alpha11\beta\cdot\alpha, \alpha\cdot\alpha11\beta)$;
- type (1): $(\alpha1\cdot\alpha\cdot\alpha1\cdot\alpha0, \alpha\cdot\alpha1\cdot\alpha)$.

We define G_{LD} to be the group $(\boldsymbol{A}\cup\boldsymbol{A}^{-1})^*/\equiv$, where $\equiv$ is the congruence generated by all LD-relations, together with all pairs $(\alpha\cdot\alpha^{-1}, \varepsilon)$ and $(\alpha^{-1}\cdot\alpha, \varepsilon)$, where ε denotes the empty word. The class of α in G_{LD} is denoted g_α.

In other words, G_{LD} is the group with presentation $\langle\{g_\alpha; \alpha\in\boldsymbol{A}\}; R_{LD}\rangle$, where R_{LD} denotes the family of all LD-relations.

Proposition 1.5 (Dehornoy [4]). *Assume that w and w' are words on $\boldsymbol{A}\cup\boldsymbol{A}^{-1}$, and the domains of the operators LD_w and $LD_{w'}$ are not disjoint. Then the following are equivalent*:

(i) *We have $(t)w = (t)w'$ for at least one term t.*

(ii) *We have* $(t)w = (t)w'$ *for every term* t *such that* $(t)w$ *and* $(t)w'$ *exist.*
(iii) *We have* $w \equiv w'$.

In the particular case when w *and* w' *are words on* $\boldsymbol{A}$, *the domains of* LD_w *and* $LD_{w'}$ *are never disjoint, and Conditions* (i) *and* (ii) *are equivalent to* $LD_w = LD_{w'}$. *Hence, the monoid* $\mathscr{G}^+_{LD}$ *is isomorphic to the submonoid* G^+_{LD} *of* G_{LD} *generated by the elements* g_α.

Let us recall that Artin's braid group B_∞ is defined as the group generated by an infinite sequence $\sigma_1, \sigma_2, \ldots$, subject to the so-called braid relations

$$\sigma_i \cdot \sigma_j = \sigma_j \cdot \sigma_i \quad \text{for } |i-j| \geq 2 \quad \text{(type (i))},$$

$$\sigma_{i+1} \cdot \sigma_i \cdot \sigma_{i+1} = \sigma_i \cdot \sigma_{i+1} \cdot \sigma_i \quad \text{(type (ii))}.$$

The deep relation between left self-distributivity and braids originates in the fact that the group B_∞ is a projection of the group G_{LD}. Indeed, the mapping

$$pr : \alpha \mapsto \begin{cases} \sigma_i & \text{for } \alpha = 1^{i-1}, \\ 1 & \text{if } \alpha \text{ contains at least one } 0, \end{cases}$$

induces a surjective homomorphism of G_{LD} onto B_∞: braid relations of type (i) are what remains from type 11 relations in G_{LD}, while braid relations of type (ii) are what remains from type 1 relations. The other LD-relations vanish, as the corresponding generators are collapsed.

As B_∞ is a homomorphic image of G_{LD}, there exists an exact sequence of groups

$$1 \to Ker(pr) \to G_{LD} \to B_\infty \to 1. \tag{1.1}$$

By definition, the kernel of pr is the normal subgroup of G_{LD} generated by the elements of the form g_α where α contains at least one 0, which happens to be also the normal subgroup of G_{LD} generated by the elements of the form $g_{0\alpha}$ [4].

2. The confluence property

We enter the core of our study. We introduce the monoid M_{LD} for which the LD-relations of Section 1 make a presentation, and we try to develop for the pair (G_{LD}, M_{LD}) the same approach as Garside and others developed for the pair (B_∞, B^+_∞), where B^+_∞ is the monoid of all positive braids. Here, we prove a first significant result about M_{LD}, namely that any two elements admit a common right multiple.

By the results of [2], we know that common right multiples always exist in the monoid $\mathscr{G}^+_{LD}$, hence, by Proposition 1.5, in the submonoid G^+_{LD} of G_{LD}. Should we know that M_{LD} embeds in G_{LD}, i.e., that M_{LD} is isomorphic to G^+_{LD}, then the existence of common right multiples in M_{LD} would follow. Now, we have no proof of the previous embedding result, so our strategy will consist in using the defining relations of M_{LD} exclusively and constructing a syntactic counterpart to the proof of the confluence property in $\mathscr{G}^+_{LD}$ as given in [2].

The monoid M_{LD} is not finitely generated, and, in contradistinction to the braid monoid B_∞^+, we cannot express it as the direct limit of a family of finitely generated submonoids. Hence, there exists in M_{LD} no direct counterpart of Garside's fundamental braids Δ_n which are crucial in the study of braids [1,6,10–12]. However, we shall see that some elements Δ_t of M_{LD} associated with the terms ∂t of [2] can be used as local versions of Δ_n.

2.1. The monoid M_{LD}

Definition. We denote by $\equiv^+$ the congruence on the monoid $\boldsymbol{A}^*$ generated by all LD-relations, and by M_{LD} the monoid $\boldsymbol{A}^*/\equiv^+$. The class of α in M_{LD} is denoted g_α^+.

Observe that $\equiv^+$ is included in $\equiv$, but there is no evidence that $\equiv^+$ be the trace of $\equiv$ on $\boldsymbol{A}^*$: the latter property is equivalent to the embeddability of the monoid M_{LD} in the group G_{LD}, and it will be discussed in Section 4 below. In the sequel, the words in $\boldsymbol{A}^*$ will be called *positive* words, as opposed to the general words of $(\boldsymbol{A} \cup \boldsymbol{A}^{-1})^*$, which are simply called words.

By Proposition 1.4, $u \equiv^+ u'$ implies $LD_u = LD_{u'}$ for all positive words u, u'. Thus, by definition, the action of $\boldsymbol{A}^*$ on T_∞ associated with the operators LD_u induces a well defined action of the monoid M_{LD} on T_∞. We can therefore use the notation LD_a for $a \in M_{LD}$ to represent the operator LD_u for an arbitrary positive word u representing a.

We begin with an easy observation.

Notation. For γ an address, and w a word on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$, we denote by γw the word obtained by shifting all addresses in w by γ, i.e., for $w = \alpha_1^{\pm 1} \cdot \ldots \cdot \alpha_p^{\pm 1}$, we define $\gamma w = (\gamma\alpha_1)^{\pm 1} \cdot \ldots \cdot (\gamma\alpha_p)^{\pm 1}$ —not to be confused with the length $p+1$ word $\gamma \cdot \alpha_1^{\pm 1} \cdot \ldots \cdot \alpha_p^{\pm 1}$.

Proposition 2.1. *For each address γ, the mapping $w \mapsto \gamma w$ induces an endomorphism sh_γ of G_{LD}, and its restriction to positive words induces an injective endomorphism sh_γ^+ of M_{LD}.*

Proof. If (w, w') is an LD-relation, so is $(\gamma w, \gamma w')$. In the case of M_{LD}, we observe in addition that, if (w, w') is an LD-relation and all members of the sequence w begin with γ, so do all generators occurring in w'. Assume that u and u' are positive words and $\gamma u \equiv^+ \gamma u'$ holds. Then, by the previous remark, all intermediate words in a sequence of elementary transformations from γu to $\gamma u'$ are of the form γv, and we obtain a sequence from u to u' by removing the prefix γ everywhere. So $u \equiv^+ u'$ holds, and sh_γ^+ is injective. $\square$

It can be proved that the endomorphisms sh_γ on G_{LD} are injective as well, but the previous simple argument does not work, as, wtarting with $\gamma w \equiv \gamma w'$, we cannot be sure that all intermediate words in a sequence of elementary transformations from γw to $\gamma w'$ are of the form γv because some factors $\alpha \cdot \alpha^{-1}\alpha$ or $\alpha^{-1} \cdot \alpha$ may appear.

Lemma 2.2. *Assume that u_1 and u_2 are positive words in $\boldsymbol{A}^*$, and every address in u_1 is orthogonal to every address in u_2. Then we have the equivalences*

$$u_1 \cdot u_2 \equiv^+ u_2 \cdot u_1, \tag{2.1}$$

$$0u_1 \cdot 0u_2 \cdot \phi \equiv^+ \phi \cdot 00u_1 \cdot 00u_2 \cdot 10u_1 \cdot 10u_2, \tag{2.2}$$

$$10u_1 \cdot 10u_2 \cdot \phi \equiv^+ \phi \cdot 01u_1 \cdot 01u_2, \tag{2.3}$$

$$11u_1 \cdot 11u_2 \cdot \phi \equiv^+ \phi \cdot 11u_1 \cdot 11u_2. \tag{2.4}$$

Proof. Use an induction on the length of u_1 and u_2. The hypothesis implies that every address in $10u_1$ is orthogonal to every address in $00u_2$, and, therefore, these addresses commute with respect to $\equiv^+$. □

2.2. Inheritance relations

Geometric reasons explain LD-relations of type 0, 10, and 11. For instance, the type 10 relation $LD_{\alpha 10\beta} \bullet LD_\alpha = LD_\alpha \bullet LD_{\alpha 01\beta}$ expresses that expanding a term at $\alpha 10\beta$, and then at α, is equivalent to expanding it at α first, and then at $\alpha 01\beta$: in both cases, we expand the βth subterm of the $\alpha 10$th subterm of t, but, if we expand at α first, then the $\alpha 10\beta$th subterm of t is moved to the address $\alpha 01\beta$ when LD_α is performed. Then the above relation expresses a skew commutativity relation where the address $\alpha 10\beta$ is replaced by what will be called its *heir* under the action of α.

In [2], more general inheritance relations are introduced, and, according to the strategy defined above, our task here will be to verify that these relations hold in M_{LD}. These technical — but easy — results are needed in the subsequent study of the elements Δ_t.

Definition. Assume that B is a set of addresses, and u is a positive word in $\boldsymbol{A}^*$. Then the set $Heir(B,u)$ of all *heirs* of elements of B under the action of LD_u is defined inductively by the following clauses:

(i) The set $Heir(B,u)$ exists if $Heir(\{\beta\},u)$ exists for every β in B, and, in this case, $Heir(B,u)$ is the union of all sets $Heir(\{\beta\},u)$ for β in B.

(ii) The set $Heir(B,\varepsilon)$ is B for every B.

(iii) If u is a single positive address say α, then $Heir(\{\beta\},\alpha)$ exists if and only if β is not a prefix of $\alpha 1$, and we have

$$Heir(\{\beta\},\alpha) = \begin{cases} \{\beta\} & \text{for } \beta \perp \alpha, \text{ or } \alpha 11 \text{ a prefix of } \beta, \\ \{\alpha 00\gamma, \alpha 10\gamma\} & \text{for } \beta = \alpha 0\gamma, \\ \{\alpha 01\gamma\} & \text{for } \beta = \alpha 10\gamma, \\ \text{undefined} & \text{for } \beta \text{ a prefix of } \alpha 1. \end{cases}$$

(iv) For $u = \alpha \cdot u_0$, α an address, $Heir(B,u)$ is $Heir(Heir(B,\alpha),u_0)$, when it exists.

The easy verification of the following results is left to the reader.

Lemma 2.3. *Assume that u is a positive word in $\boldsymbol{A}^*$, and β is an address.*

(i) *The set $Heir(\{\beta\},u)$ exists if some address in the outline of the term t_u^{L} is a prefix of β.*

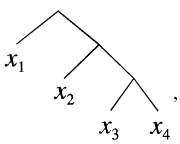
(ii) *If $Heir(\{\beta\},u)$ is defined, so is $Heir(\{\beta\gamma\},u)$ for every γ, and the latter set is equal to the set of all addresses $\beta'\gamma$ for β' in $Heir(\{\beta\},u)$.*

(iii) *The elements of every set of the form $Heir(\{\beta\},u)$ are pairwise orthogonal.*

(iv) *Assume that LD_u maps the term t to the term t', and β belongs to the skeleton of t. If $Heir(\{\beta\},u)$ is defined, then $sub(t',\beta') = sub(t,\beta)$ holds for every β' in $Heir(\{\beta\},u)$.*

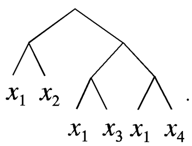
Observe that Point (iv) always applies when the address β lies in the outline of the term t, i.e., when β is the address of a variable in t; then $Heir(\{\beta\},u)$ is the family of those occurrences in the outline of the term t' that come from β in t, in an obvious sense. In particular, if the variable x occurs at β and only there in t, then $Heir(\{\beta\},u)$ is exactly the set of those addresses where x occurs in t'.

Example 2.4. Consider the case $u = \phi \cdot 1$. The term $t_{\phi\cdot 1}^{L}$ is the canonical term



,

which is mapped to



.

Hence, those addresses β for which $Heir(\{\beta\},\phi\cdot 1)$ is not defined are $\phi, 1$ and 11. The reader can check that $Heir(\{0\},\phi\cdot 1)$ is $\{00, 100, 110\}$, which corresponds to the fact that the variable x_1 occurring at 0 in the first term has three copies with addresses 00,100 and 110 in the second one. Similarly, $Heir(\{10\},\phi\cdot 1)$ is $\{01\}$, while $Heir(\{110\},\phi\cdot 1)$ is $\{101\}$, and $Heir(\{111\},\phi\cdot 1)$ is $\{111\}$. Lemma 2.3(ii) implies $Heir(\{0\gamma\},\phi\cdot 1) = \{00\gamma, 100\gamma, 110\gamma\}$ for every address γ.

Using the techniques of [2], one can prove that, if u is a positive word in $\boldsymbol{A}^*$, β is an address, and $Heir(\{\beta\},u)$ is defined, then we have

$$LD_\beta \bullet LD_u = LD_u \bullet \prod_{\beta' \in Heir(\{\beta\},u)} LD_{\beta'} \tag{2.5}$$

According to our strategy, we shall establish a syntactic counterpart to (2.5), namely:

Proposition 2.5. *Assume that u is a positive word in A^*, β is an address, and that $Heir(\{\beta\}, u)$ is defined. Then we have the equivalence*

$$\beta \cdot u \equiv^+ u \cdot \prod_{\beta' \in Heir(\{\beta\},u)} \beta' \tag{2.6}$$

Proof. We use induction on the length of u. The result is trivial when u is empty. If u has length 1, the result corresponds to LD-relations respectively of types $(\perp), (0)$, (10) and (11). Otherwise, assume $u = \alpha \cdot u_0$, where α is an address. By construction, the hypothesis that the set $Heir(\{\beta\}, u)$ exists implies that the sets $Heir(\{\beta\}, \alpha)$ and $Heir(Heir(\{\beta\}, \alpha), u_0)$ exist, and that the latter is equal to $Heir(\{\beta\}, u)$. By induction hypothesis, we have

$$\beta \cdot \alpha \equiv^+ \alpha \cdot \prod_{\beta' \in Heir(\{\beta\},\alpha)} \beta'$$

and, therefore,

$$\beta \cdot u \equiv^+ \alpha \cdot \prod_{\beta' \in Heir(\{\beta\},\alpha)} \beta' \cdot u_0.$$

Now, by induction hypothesis again, we have, for each address β' in the set $Heir(\{\beta\}, \alpha)$,

$$\beta' \cdot u_0 \equiv^+ u_0 \cdot \prod_{\beta'' \in Heir(\{\beta'\},u_0)} \beta''$$

and we obtain

$$\beta \cdot u \equiv^+ \alpha \cdot u_0 \cdot \prod_{\beta' \in Heir(\{\beta\},\alpha)} \prod_{\beta'' \in Heir(\{\beta'\},u_0)} \beta''. \tag{2.7}$$

By Lemma 2.3(iii), the addresses β' in $Heir(\{\beta\}, \alpha)$ are pairwise orthogonal, so Lemma 2.2 tells us that the involved addresses β'' commute up to $\equiv^+$, and the double product in (2.7) is also $\equiv^+$-equivalent to the product $\prod_{\beta' \in Heir(\{\beta\},u)} \beta'$ of (2.5). $\square$

2.3. Uniform distribution relations

Another type of geometric relation in the monoid $\mathscr{G}_{LD}^+$ generalizes the type 1 LD-relations. We first introduce an auxiliary operation on T_∞.

Definition. Assume that t_0 is a term. For t in T_∞, the term $t_0 * t$ is defined inductively by the clauses: $t_0 * t = t_0 \cdot t$ if t is a variable, $t_0 \cdot t = (t_0 * t_1) \cdot (t_0 * t_2)$ for $t = t_1 \cdot t_2$.

The term $t_0 * t$ is obtained from $t_0 \cdot t$ by distributing t_0 everywhere down to the level of the leaves in the tree associated with t: more formally, $t_0 * t$ is the substitute t^h, where $h(x_i)$ is defined to be $t_0 \cdot x_i$ for every variable x_i. An induction shows that, for all terms t_0, t, the term $t_0 * t$ is an LD-expansion of the term $t_0 \cdot t$, and it is easy to construct a positive word describing the way this LD-expansion is performed.

Definition. For t a term, the word δ_t is defined inductively by $\delta_t = \varepsilon$ for t a variable, and $\delta_t = \phi \cdot 1\delta_{t_2} \cdot 0\delta_{t_1}$ for $t = t_1 \cdot t_2$.

The inductive definition implies that the word δ_t is obtained by taking the product of all addresses that belong to the skeleton of t but not to the outline of t according to the unique linear ordering of addresses satisfying $\gamma < \gamma 1\alpha < \gamma 0\beta$ for all α, β, γ. An easy verification gives

Lemma 2.6. *For all terms t_0, t, we have $t_0 * t = (t_0 \cdot t)\delta_t$.*

The methods of [2] imply that, if u is a positive word in $\boldsymbol{A}^*$, and the operator LD_u maps the term t to the term t', then we have

$$LD_{\delta_t} \bullet LD_u = LD_{1u} \bullet LD_{\delta_{t'}}. \tag{2.8}$$

Again, the geometric idea is simple. Applying LD_{δ_t} replaces the term $t_0 \cdot t$ with the term t^h where h is the substitution defined by $h(x_i) = t_0 \cdot x_i$. If LD_u maps t to t', then LD_{1u} maps $t_0 \cdot t$ to $t_0 \cdot t'$, and LD_u maps also t^h to t'^h. Now t'^h is the result of replacing every variable in t' by its product with t_0, i.e., it is the term $t_0 * t'$, hence the result of applying $LD_{\delta_{t'}}$ to $t_0 \cdot t'$.

As above, we establish a syntactic counterpart to (2.8).

Proposition 2.7. *Assume that u is a positive word, and LD_u maps t to t'. Then we have*

$$\delta_t \cdot u \equiv^+ 1u \cdot \delta_{t'}. \tag{2.9}$$

Proof. We use induction on the length of the word u. Assume first that u has length 1, i.e., u is a single address say α. We argue inductively on the length of the address α. Assume first $\alpha = \phi$. So we assume $t' = (t)\phi$, and prove $\delta_t \cdot \phi \equiv^+ 1 \cdot \delta_{t'}$. The hypothesis that $(t)\phi$ is defined implies that t can be decomposed into $t_0 \cdot (t_1 \cdot t_2)$. Now we have

$$\begin{aligned}
\delta_t \cdot \phi &= \phi \cdot 1 \cdot 11\delta_{t_2} \cdot 10\delta_{t_1} \cdot 0\delta_{t_0} \cdot \phi \\
&\equiv^+ \phi \cdot 1 \cdot 11\delta_{t_2} \cdot 10\delta_{t_1} \cdot \phi \cdot 10\delta_{t_0} \cdot 00\delta_{t_0} \quad \text{(type 0)} \\
&\equiv^+ \phi \cdot 1 \cdot 11\delta_{t_2} \cdot \phi \cdot 01\delta_{t_1} \cdot 10\delta_{t_0} \cdot 00\delta_{t_0} \quad \text{(type 10)}
\end{aligned}$$

$$\equiv^+ \phi \cdot 1 \cdot \phi \cdot 11\delta_{t_2} \cdot 01\delta_{t_1} \cdot 10\delta_{t_0} \cdot 00\delta_{t_0} \qquad \text{(type 11)}$$

$$\equiv^+ \phi \cdot 1 \cdot \phi \cdot 11\delta_{t_2} \cdot 10\delta_{t_0} \cdot 01\delta_{t_1} \cdot 00\delta_{t_0} \qquad \text{(type } \perp)$$

$$\equiv^+ 1 \cdot \phi \cdot 1 \cdot 0 \cdot 11\delta_{t_2} \cdot 10\delta_{t_0} \cdot 01\delta_{t_1} \cdot 00\delta_{t_0} \qquad \text{(type 1)}$$

$$\equiv^+ 1 \cdot \phi \cdot 1 \cdot 11\delta_{t_2} \cdot 10\delta_{t_0} \cdot 0 \cdot 01\delta_{t_1} \cdot 00\delta_{t_0} = 1 \cdot \delta_{t'} \qquad \text{(type } \perp).$$

Assume now $\alpha = 0\beta$. Then, writing $t = t_0 \cdot t_1$ and $t' = t'_0 \cdot t_1$, we have $t'_0 = (t_0)\beta$, and the induction hypothesis gives $\delta_{t_0} \cdot \beta \equiv^+ 1\beta \cdot \delta_{t'_0}$. By Lemma 2.1, this implies $0\delta_{t_0} \cdot 0\beta \equiv^+ 01\beta \cdot 0\delta_{t'_0}$, and we deduce

$$\begin{aligned} \delta_t \cdot \alpha = \phi \cdot 1\delta_{t_1} \cdot 0\delta_{t_0} \cdot 0\beta &\equiv^+ \phi \cdot 0\delta_{t_0} \cdot 0\beta \cdot 1\delta_{t_1} && \text{(type } \perp) \\ &\equiv^+ \phi \cdot 01\beta \cdot 0\delta_{t'_0} \cdot 1\delta_{t_1} \\ &\equiv^+ 10\beta \cdot \phi \cdot 0\delta_{t'_0} \cdot 1\delta_{t_1} = 1\alpha \cdot \delta_{t'}. && \text{(type 10)} \end{aligned}$$

The argument is similar for $\alpha = 1\beta$, and the induction on the length of u is easy. □

2.4. The confluence property

It has been proved in [6] that any two LD-expansions of a given term admit a common LD-expansion. In the current framework, this means that, if t is a term and u, v are two positive words such that both $(t)u$ and $(t)v$ exist, then there exist words u' and v' – possibly depending on t – such that the LD-expansions $(t)uv'$ and $(t)vu'$ exist and are equal. This implies that the operators $LD_{uv'}$ and $LD_{vu'}$ are equal, and, therefore, makes the equivalence $uv' \equiv^+ vu'$ plausible. Here we shall establish a strong form of this result.

Our syntactic proof will follow the proof of [2], which consists in introducing, for every term t, a distinguished term ∂t which is a common LD-expansion of all basic LD-expansions of t.

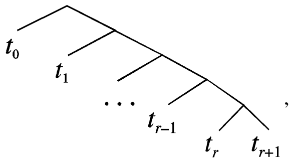
Definition (Dehornoy [2])**.** For t a term, we define inductively the term ∂t by

$$\partial t = \begin{cases} t & \text{if } t \text{ is a variable,} \\ \partial t_0 * \partial t_1 & \text{for } t = t_0 \cdot t_1. \end{cases}$$

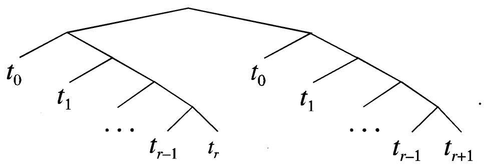
By construction, the term ∂t is an LD-expansion of the term t for every t. The idea is to select a positive word $\boldsymbol{\Delta}_t$ such that ∂t is the LD-expansion $(t)\boldsymbol{\Delta}_t$, and then to use $\boldsymbol{\Delta}_t$ as a syntactic counterpart of ∂t.

Definition. For $\alpha \in \boldsymbol{A}$, we put $\alpha^0 = \varepsilon$, and $\alpha^{(r)} = \alpha 1^{r-1} \cdot \alpha 1^{r-2} \cdot \cdots \cdot \alpha 1 \cdot \alpha$ for $r \geq 1$.

Example 2.8. By construction, $(t)\phi^{(r)}$ is defined if and only if 1^r0 belongs to the skeleton of t, i.e., if $ht_{\mathrm{R}}(t) \geq r+1$. holds. Then t has the form



and $(t)\phi^{(r)}$ is



Lemma 2.9. *Assume* $ht_{\mathrm{R}}(t) = r+1$. Let $s_0 \cdot s_1 = (t)\phi^{(r)}$. *Then we have* $\partial t = \partial s_0 \cdot \partial s_1$.

Proof. Assume $t = t_0 \cdot t_1$. We use induction on r. For $r = 0$, t_1 is a variable, say x, we have $\partial(t_0 \cdot x) = \partial t_0 \cdot x$, and the result is obvious. Otherwise, we have $ht_{\mathrm{R}}(t_1) = r$. Let $s_{10} \cdot s_{11} = (t_1)\phi^{(r-1)}$. By induction hypothesis, we have $\partial t_1 = \partial s_{10} \cdot \partial s_{11}$, so we deduce

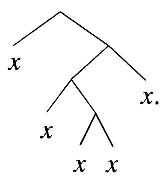
$$\partial t = \partial t_0 * (\partial s_{10} \cdot \partial s_{11}) = (\partial t_0 * \partial s_{10}) \cdot (\partial t_0 * \partial s_{11}) = \partial(t_0 \cdot s_{10}) \cdot \partial(t_0 \cdot s_{11}).$$

Now, by construction, we have $s_e = t_e \cdot s_{1e}$ for $e = 0, 1$. $\square$

Definition. Assume that t is a term. Then the word Δ_t is defined by

$$\Delta_t = \begin{cases} \varepsilon & \text{if } t \text{ is a variable,} \\ \phi^{(r)} \cdot 1\Delta_{s_1} \cdot 0\Delta_{s_0} & \text{otherwise, with } s_0 \cdot s_1 = (t)\phi^{(r)} \text{ and } r+1 = ht_{\mathrm{R}}(t). \end{cases}$$

Example 2.10. Let t be the term



We have $ht_{\mathrm{R}}(t) = 2$, so the exponent of ϕ in Δ_t will be $2-1=1$. The right subterm of the image of t under LD_ϕ is the term $s_1 = x^{[2]}$, while its left subterm is $s_0 = x^{[4]}$, where $x^{[k]}$ denotes the kth right power of x inductively defined by $x^{[1]} = x$, and $x^{[k]} = x \cdot x^{[k-1]}$ for $k \geq 2$. Then, we have $\partial s_1 = s_1$, hence $\Delta_{s_1} = \varepsilon$. Now, we have $ht_{\mathrm{R}}(s_0) = 3$, so the exponent of ϕ in Δ_{s_0} is $3-1=2$. The right and left subterms of $(s_0)\phi^{(2)}$ are

$s_{10} = s_{00} = x^{[3]}$. We have $ht_{\mathrm{R}}(s_{00}) = 2$, so the exponent of ϕ in $\varDelta_{s_{00}}$ is $2 - 1 = 1$. The right and left subterms of the image of s_{00} under LD_ϕ are $x^{[2]}$, so we are done. By gathering the elements, we find

$$\varDelta_t = \phi \cdot 0\varDelta_{s_0} = \phi \cdot 0^{(2)} \cdot 01\varDelta_{s_{10}} \cdot 00\varDelta_{s_{00}} = \phi \cdot 0^{(2)} \cdot 01 \cdot 00.$$

Applying Lemma 2.9, we obtain the following result immediately:

Proposition 2.11. *For every term t is a term, we have $(t)\varDelta_t = \partial t$.*

We shall establish in the sequel that the words $\varDelta_t$ share many technical properties with Garside's fundamental braid words $\varDelta_n$. We begin with some preliminary results.

Lemma 2.12. *Assume $t = t_0 \cdot t_1$. Then we have*

$$\varDelta_t \equiv^+ 1\varDelta_{t_1} \cdot 0\varDelta_{t_0} \cdot \delta_{\partial t_1}, \tag{2.10}$$

$$\varDelta_t \equiv^+ 0\varDelta_{t_0} \cdot \delta_{t_1} \cdot \varDelta_{t_1}, \tag{2.11}$$

$$\varDelta_t \equiv^+ \delta_{t_1} \cdot \prod_{\alpha \in Out(t_1)} \alpha 0\varDelta_{t_0} \cdot \varDelta_{t_1}. \tag{2.12}$$

Proof. We prove (2.10) using induction on t_1. Let $r + 1 = ht_{\mathrm{R}}(t)$ and $s_0 \cdot s_1 = (t)\phi^{(r)}$. If t_1 is a variable, then we have $\partial t_1 = t_1$, $r = 0$, hence $s_0 = t_0$, $s_1 = t_1$. By definition, we have $\varDelta_t = 0\varDelta_{t_0}$, and (2.10) is an equality. Otherwise, assume $t_1 = t_{10} \cdot t_{11}$. We have $ht_{\mathrm{R}}(t_1) = r$. Let $s_{10} \cdot s_{11} = (t_1)\phi^{(r-1)}$. By construction, we have $s_1 = t_0 \cdot s_{11}$ and $s_0 = t_0 \cdot s_{10}$. The sizes of the right subterms of s_1 and s_0, namely s_{11} and s_{10}, are strictly smaller than the size of the right subterm of t, namely t_1, so the induction hypothesis gives

$$\varDelta_{s_1} \equiv^+ 1\varDelta_{s_{11}} \cdot 0\varDelta_{t_0} \cdot \delta_{\partial s_{11}} \quad \text{and} \quad \varDelta_{s_0} \equiv^+ 1D_{s_{10}} \cdot 0\varDelta_{t_0} \cdot \delta_{\partial s_{10}}$$

and we deduce

$$\varDelta_t \equiv^+ \phi^{(r)} \cdot 11\varDelta_{s_{11}} \cdot 10\varDelta_{t_0} \cdot 1\delta_{\partial s_{11}} \cdot 01\varDelta_{s_{10}} \cdot 00\varDelta_{t_0} \cdot 0\delta_{\partial s_{10}}.$$

Using type $(\perp)$ relations, this can be rearranged into

$$\varDelta_t \equiv^+ \phi^{(r)} \cdot 11\varDelta_{s_{11}} \cdot 01\varDelta_{s_{10}} \cdot 10\varDelta_{t_0} \cdot 00\varDelta_{t_0} \cdot 1\delta_{\partial s_{11}} \cdot 0\delta_{\partial s_{10}}.$$

Now, we have $\phi^{(r)} = 1^{(r-1)} \cdot \phi$, and using successively LD-relations of types (11), (10) and (0), we push the factor ϕ to the right, thus obtaining

$$\varDelta_t \equiv^+ 1^{(r-1)} \cdot 11\varDelta_{s_{11}} \cdot 10\varDelta_{s_{10}} \cdot 0\varDelta_{t_0} \cdot \phi \cdot 1\delta_{\partial s_{11}} \cdot 0\delta_{\partial s_{10}}.$$

Then we have $1^{(r-1)} \cdot 11\varDelta_{s_{11}} \cdot 10\varDelta_{s_{10}} = 1\varDelta_{s_{10} \cdot s_{11}} = 1\varDelta_{t_1}$, and $\phi \cdot 1\delta_{\partial s_{11}} \cdot 0\delta_{\partial s_{10}} = \delta_{\partial t_1}$, and we have obtained (2.10).

The other formulas follow easily. Indeed, we deduce (2.11) from (2.10) by using Proposition 2.7, since, by construction, $LD_{\varDelta_{t_1}}$ maps t_1 to ∂t_1. We deduce (2.12) from

(2.11) by using Proposition 2.5, since, by construction again, the set $Heir(\{0\}, \delta_{t_1})$ exists and is equal to the set of all addresses $\beta 0$ for β in the outline of t_1. $\square$

Remark. Let u be the word involved in the right-hand side of (2.10). The diagram

$$t = t_0 \cdot t_1 \xmapsto{LD_{1\Delta_{t_1}}} t_0 \cdot \partial t_1 \xmapsto{LD_{0\Delta_{t_0}}} \partial t_0 \cdot \partial t_1 \xmapsto{LD_{\partial t_1}} \partial t_0 * \partial t_1 = \partial t$$

makes it obvious that the operator LD_u maps the term t to the term ∂t, which implies that the operators LD_{Δ_t} and LD_u coincide. However, the equivalence $\Delta_t \equiv^+ u$ is a stronger result.

Now, we follow the approach of [2]. The first result is that the term ∂t is an LD-expansion of every basic LD-expansion of t. Its syntactic counterpart is the following result:

Lemma 2.13. *Assume that α is an address and the term t belongs to the domain of the operator LD_α. Then there exists a positive word u satisfying $\alpha \cdot u \equiv^+ \Delta_t$.*

Proof. We use induction on α. For $\alpha = \phi$, the result follows from Formula (2.12), which gives a word that explicitly begins with ϕ provided that the right subterm t_1 of t exists, i.e., t is not a variable, and δ_{t_1} is not empty, i.e., t_1 is not a variable, so for $ht_R(t) \geq 2$, which is the case if $(t)\phi$ exists. Otherwise, assume $\alpha = 0\beta$ and $t = t_0 \cdot t_1$. Formula (2.10) shows that Δ_t is $\equiv^+$-equivalent to a word that begins with $0\Delta_{s_0}$. By construction, the term t_0 lies in the domain of the operator LD_β, so, by induction hypothesis, Δ_{t_0} is $\equiv^+$-equivalent to a positive word of the form $\beta \cdot u_0$, and we obtain

$$\Delta_t \equiv^+ \alpha \cdot 0u_0 \cdot 1\Delta_{t_1} \cdot \delta_{\partial t_1}.$$

Assume now $\alpha = 1\beta$. The argument is similar, since, at the expense of using additional type ($\perp$) relations, we have also $\Delta_t \equiv^+ 1\Delta_{t_1} \cdot 0\Delta_{t_0} \cdot \delta_{\partial t_1}$. $\square$

The next step is the counterpart to the fact that the operator ∂ is increasing with respect to LD-expansion: if t' is an LD-expansion of t, then $\partial t'$ is an LD-expansion of ∂t.

Lemma 2.14. *Assume that the operator LD_α maps t* to *t'. Then there exists a positive word u satisfying $\alpha \cdot \Delta_{t'} \equiv^+ \Delta_t \cdot u$.*

Proof. We begin with the case $\alpha = \phi$. We argue inductively on the size of the 11-subterm of t, which must exist as $(t)\phi$ does. Write $t = t_0 \cdot (t_1 \cdot t_2)$. Assume first that t_2 is a variable. Then we have $ht_R(t) = 2$, hence

$$\Delta_t = \phi \cdot 1\Delta_{s_1} \cdot 0\Delta_{s_0}, \tag{2.13}$$

with $s_0 = t_0 \cdot t_1$ and $s_1 = t_0 \cdot t_2$. But, then, s_0 is the left subterm of t', and s_1 is its right subterm. So, by Formula (2.10), we have

$$\Delta_t \equiv^+ 1\Delta_{s_1} \cdot 0\Delta_{s_0} \cdot \delta_{\partial s_1}. \tag{2.14}$$

By comparing (2.13) and (2.14), we obtain $\phi \cdot \Delta_{t'} \equiv^+ \Delta_t \cdot \delta_{\partial s_1}$, which has the expected form.

Assume now that t_2 is not a variable. Let $r+1 = ht_{\mathrm{R}}(t)$ and $s_0 \cdot s_1 = (t)\phi^{(r)}$, and let similarly $s'_0 \cdot s'_1 = (t')\phi^{(r)}$. By definition, and using $ht_{\mathrm{R}}(t) = ht_{\mathrm{R}}(t')$, we have

$$\Delta_t = \phi^{(r)} \cdot 1\Delta_{s_1} \cdot 0\Delta_{s_0}, \tag{2.15}$$

$$\Delta_{t'} = \phi^{(r)} \cdot 1\Delta_{s'_1} \cdot 0\Delta_{s'_0}. \tag{2.16}$$

By construction, we have $s'_1 = (s_1)\phi$ and $s'_0 = (s_0)\phi$, as is verified by writting $t = t_0 \cdot t_1 \cdot \ldots \cdot t_r \cdot x$, where x is a variable. Moreover, the size of the 11th subterms of s_1 and s_0 are strictly smaller than the size of the 11th subterm of t. So, by induction hypothesis, there exist positive words u_1, u_0 satisfying $\phi \cdot \Delta_{s'_e} \equiv^+ \Delta_{s_e} \cdot u_e$ for $e = 1, 0$. Then, an induction gives the equivalence

$$\phi \cdot \phi^{(r)} \equiv^+ \phi^{(r)} \cdot 1 \cdot 0$$

for $r \geq 2$: the basic case is $r = 2$, where it is a type 1 relation. So, we obtain

$$\begin{aligned}
\phi \cdot \Delta_{t'} = \phi \cdot \phi^{(r)} \cdot 1\Delta_{s'_1} \cdot 0\Delta_{s'_0} &\equiv^+ \phi^{(r)} \cdot 1 \cdot 1\Delta_{s'_1} \cdot 0 \cdot 0\Delta_{s'_0} \\
&\equiv^+ \phi^{(r)} \cdot 1\Delta_{s_1} \cdot 1u_1 \cdot 0\Delta_{s_0} \cdot 0u_0 \\
&\equiv^+ \phi^{(r)} \cdot 1\Delta_{s_1} \cdot 0\Delta_{s_0} \cdot 1u_1 \cdot 0u_0 = \Delta_t \cdot 1u_1 \cdot 0u_0,
\end{aligned}$$

and we are done.

Assume now $\alpha = 0\beta$. Write $t = t_0 \cdot t_1$. We have $t' = t'_0 \cdot t_1$ with $t'_0 = (t_0)\beta$. By induction hypothesis, there exists a positive word u_0 satisfying $\beta \cdot \Delta_{t'_0} \equiv^+ \Delta_{t_0} \cdot u_0$. Starting from (2.10), we obtain

$$\begin{aligned}
\alpha \cdot \Delta_{t'} &\equiv^+ \alpha \cdot 0\Delta_{t'_0} \cdot 1\Delta_{t_1} \cdot \delta_{\partial t_1} \equiv^+ 0\beta \cdot \Delta_{t'_0} \cdot 1\Delta_{t_1} \cdot \delta_{\partial t_1} \\
&\equiv^+ 0\Delta_{t_0} \cdot u_0 \cdot 1\Delta_{t_1} \cdot \delta_{\partial t_1} \\
&\equiv^+ 0\Delta_{t_0} \cdot 1\Delta_{t_1} \cdot 0u_0 \cdot \delta_{\partial t_1} \\
&\equiv^+ 0\Delta_{t_0} \cdot 1\Delta_{t_1} \cdot \delta_{\partial t_1} \cdot \prod_{\alpha \in Out(t_1)} \alpha 0 u_0 \quad \text{(by Proposition 2.5)} \\
&\equiv^+ \Delta_t \cdot \prod_{\alpha \in Out(t_1)} \alpha 0 u_0.
\end{aligned}$$

Assume finally $\alpha = 1\beta$. We have $t' = t_0 \cdot t'_1$, with $t'_1 = (t_1)\beta$. By induction hypothesis, we have $\beta \cdot \Delta_{t'_1} \equiv^+ \Delta_{t_1} \cdot u_1$ for some positive word u_1. We deduce

$$\begin{aligned}\alpha \cdot \Delta_{t'} &\equiv^+ \alpha \cdot 0\Delta_{t_0} \cdot 1\Delta_{t'_1} \cdot \delta_{\partial t_1} \equiv^+ 0\Delta_{t_0} \cdot 1\beta \cdot \Delta_{t'_1} \cdot \delta_{\partial t_1} \\ &\equiv^+ 0\Delta_{t_0} \cdot 1\Delta_{t_1 \cdot u_1} \cdot \delta_{\partial t_1} \\ &\equiv^+ 0\Delta_{t_0} \cdot 1\Delta_{t_1} \cdot 1u_1 \cdot \delta_{\partial t_1} \\ &\equiv^+ 0\Delta_{t_0} \cdot 1\Delta_{t_1} \cdot \delta_{\partial t_1} \cdot u_1 \quad \text{(by Proposition 2.7)} \\ &\equiv^+ \Delta_t \cdot u_1. \qquad \square\end{aligned}$$

Remark. Not only does the previous proof show the existence of a positive word u satisfying $\phi \cdot \Delta_{t'} \equiv^+ \Delta_t \cdot u$, but it also gives an inductive formula for constructing such a word, namely

$$u = \prod_{\alpha \in Out(t_2)} \alpha\phi \cdot 0\delta_{\partial t_0}$$

for $t = t_0 \cdot t_1 \cdot t_2$ and $t' = (t)\phi$. This formula is easily understandable: ∂t is obtained from ∂t_2 by substituting every variable x with $\partial t_0 * (\partial t_1 \cdot x)$, i.e., $\partial(t_0 * \partial t_1) \cdot (\partial t_0 \cdot x)$, while $\partial t'$ is obtained from ∂t_2 by substituting every variable x with $(\partial t_0 * \partial t_1) * (\partial t_0 \cdot x)$, i.e., $\partial(t_0 * \partial t_1) * (\partial t_0 \cdot x)$. So $\partial t'$ is obtained from ∂t by applying the operator $LD_{\phi \cdot 0\delta_{\partial t_0}}$ at each address in the outline of the term ∂t_{11}.

Lemma 2.15. *Assume that u is a positive word in A^*, and LD_u maps the term t to the term t'. Then there exists a positive word u' satisfying*

$$u \cdot \Delta_{t'} \equiv^+ \Delta_t \cdot u'. \tag{2.17}$$

Proof. We use induction on the length of u. For u empty, the result is trivial. For u of length 1, the result is Lemma 2.14. Otherwise, assume $u = u_1 \cdot u_2$ where neither u_1 nor u_2 is empty. Let $t_1 = (t)u_1$. By induction hypothesis, there exist words u'_1, u'_2 satisfying $u_e \cdot \Delta_{t_1} \equiv^+ \Delta_t \cdot u'_e$ for $e = 1, 2$. We deduce

$$u \cdot \Delta_{t'} \equiv^+ u_1 \cdot \Delta_{t_1} \cdot u'_2 \equiv^+ \Delta_t \cdot u'_1 \cdot u'_2. \qquad \square$$

We turn now to the most general case, and, to this end, we iterate the construction of the words Δ_t.

Definition. For t a term, we put $\Delta_t^{(0)} = \varepsilon$, and $\Delta_t^{(k)} = \Delta_t \cdot \Delta_{\partial t} \cdot \dots \cdot \Delta_{\partial^{k-1} t}$ for $k \geq 1$.

Lemma 2.16. *Assume that u is a positive word of length at most k and the term t lies in the domain of the operator LD_u. Then there exists a positive word v' satisfying $u \cdot v' \equiv^+ \Delta_t^{(k)}$.*

Proof. (Fig. 1). We use induction on k. The result is trivial for $k=0$. Otherwise, write $u=u_0\cdot\alpha$, where α is an address. By induction hypothesis, there exists a positive word v_0 satisfying $u_0\cdot v_0\equiv^+ \Delta_t^{(k-1)}$. Let t' be the image of t under LD_{u_0}. By hypothesis, t' lies in the domain of LD_α, so, by Lemma 2.14, there exists a positive word v satisfying $\alpha\cdot v'\equiv^+ \Delta_{t'}$. Applying Lemma 2.15 to the terms t' and $\partial^{k-1}t$, we see that there exists a positive word v_0' satisfying $v_0\cdot\Delta_{\partial^{k-1}t}\equiv^+\Delta_{t'}\cdot v_0'$. We deduce

$$\begin{aligned} u\cdot v'\cdot v_0' &= u_0\cdot\alpha\cdot v'\cdot v_0'\equiv^+ u_0\cdot\Delta_{t'}\cdot v_0' \\ &\equiv^+ u_0\cdot v_0\cdot\Delta_{\partial^{k-1}t}\equiv^+\Delta_t^{(k-1)}\cdot\Delta_{\partial^{k-1}t}=\Delta_t^{(k)}, \end{aligned}$$

hence taking $u'=v'\cdot v_0'$ gives the result. □

We are now ready to conclude. We have mentioned above that, for each positive word u, the domain of the operator LD_u consists of all substitutes of some well defined canonical term t_u^{L}. This result extends to the case of several operators: if u and v are positive words, the intersection of the domains of LD_u and LD_v is the set of all substitutes of some unique canonical term $t_{u,v}^{\mathrm{L}}$. We can now state the following strong form of confluence:

Proposition 2.17. *Assume that u, v are positive words of length at most k in A^*. Let $t=t_{u,v}^{\mathrm{L}}$. Then there exist positive words u', v', satisfying*

$$u\cdot v'\equiv^+ v\cdot u'\equiv^+\Delta_t^{(k)}. \tag{2.18}$$

Proof. Applying Lemma 2.16 to $t_{u,v}^{\mathrm{L}}$ gives two positive words u', v' such that both $u\cdot v'$ and $v\cdot u'$ are $\equiv^+$-equivalent to $\Delta_t^{(k)}$. □

Observe that, in the above situation, the domain of the operators $LD_{u\cdot v'}$ and $LD_{v\cdot u'}$ is the intersection of the domains of LD_u and LD_v, i.e., we have found a common right multiple for u and v such that the associated operator has the largest possible domain.

By projecting the result of Proposition 2.17 to M_{LD}, we obtain

Proposition 2.18. *Any two elements of the monoid M_{LD} admit a common right multiple.*

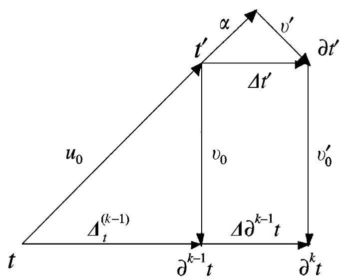


Fig. 1. Proof of Lemma 2.16.

Let us observe that, LD-relations, in contradistinction to braid relations, are not symmetric, so the results involving right multiples do not automatically imply a counterpart for left multiples. A typical example is the property that any two elements of M_{LD} always admit a common right multiple. The symmetric property about left multiples is false. Indeed, let us consider the positive words $u = \phi \cdot 0$ and $v = \phi$. It is easy to check that the domain of the operator $LD_{\phi \cdot 0 \cdot \phi^{-1}}$ is empty, which implies that no equality $u_1 \cdot \phi \cdot 0 \equiv^+ v_1 \cdot \phi$ may hold in $\boldsymbol{A}^*$, i.e., the elements $g_\phi^+ g_0^+$ and g_ϕ^+ admit no common left multiple in the monoid M_{LD}.

3. Simple elements in M_{LD}

The next step in our study of the monoid M_{LD} consists in applying the word reversing method of [6,17] Some results in this direction have already been mentioned in [4], so we shall just briefly recall the principles.

3.1. Word reversing

Both the braid relations and the LD-relations have the particular syntactical property that, for each pair of generators x, y, there exists in the considered list of relations exactly one relation of the type $x \cdot \ldots = y \cdot \ldots$, i.e., one relation that prescribes how to complete x and y on the right so as to obtain a common right multiple. With the definitions of [6], this means that these presentations are associated with a complement on the right. Indeed, let us define, for i, j in $\boldsymbol{N}$,

$$f(\sigma_i, \sigma_j) = \begin{cases} \sigma_j & \text{for } |i-j| \geq 2, \\ \sigma_j \cdot \sigma_i & \text{for } |i-j| = 1, \\ \varepsilon & \text{for } i = j \end{cases}$$

and, for α, β in $\boldsymbol{A}$ (the set of all binary addresses),

$$f(\alpha, \beta) = \begin{cases} \alpha 10\gamma \cdot \alpha 00\gamma & \text{for } \beta = \alpha 0\gamma, \\ \alpha 01\gamma & \text{for } \beta = \alpha 10\gamma, \\ \beta \cdot \alpha & \text{for } \beta = \alpha 1, \\ \varepsilon & \text{for } \alpha = \beta, \\ \beta \cdot \alpha \cdot \beta 0 & \text{for } \alpha = \beta 1, \\ \alpha & \text{in all other cases, i.e., if } \alpha \text{ is not a prefix of } \beta 1, \\ & \text{or if } \alpha 11 \text{ is a prefix of } \beta. \end{cases}$$

Then, the positive braid congruence that presents the braid monoid B_∞^+ is the congruence on the monoid BW_∞ of all words on the alphabet $\{\sigma_1, \sigma_2, \ldots\}$ generated by those pairs of the form $(\sigma_i \cdot f(\sigma_i, \sigma_j), \sigma_j \cdot f(\sigma_j, \sigma_i))$, and, similarly, the congruence $\equiv^+$ that presents the monoid M_{LD} as a quotient of $\boldsymbol{A}^*$ is generated by all pairs of the form $(\alpha \cdot f(\alpha, \beta), \beta \cdot f(\beta, \alpha))$. In the sequel, we shall refer to the previous mappings as the braid complement and the LD complement respectively.

We have observed that the mapping pr that maps α to σ_{i+1} when α is of the form 1^i, and to ε otherwise, induces a surjective homomorphism of the monoid M_{LD} onto the braid monoid B_∞^+. We observe now that the mapping pr preserves the right complements as well.

Lemma 3.1. *The projection pr of $(\boldsymbol{A} \cup \boldsymbol{A}^{-1})^*$ onto BW_∞ preserves the right complements, in the sense that the equality*

$$pr(f(\alpha, \beta)) = f(pr(\alpha), pr(\beta)) \tag{3.1}$$

holds for all addresses α, β.

The direct verification is straightforward.

The fact that the presentations of B_∞^+ and of M_{LD} are associated with right complements is not powerful in itself, and strong results can be deduced only when the complements satisfy some additional hypotheses called atomicity and coherence [6,8]. In order to introduce them, we recall some definitions.

Assume that X is an arbitrary set, and f is a mapping on $X \times X$ into the free monoid X^* generated by X such that $f(x,x)$ is the empty word for every x in X. Let $(X \cup X^{-1})^*$ denote the set of all words over the union of X and a disjoint copy X^{-1} of X, $X^{-1} = \{x^{-1}; x \in X\}$. For w in $(X \cup X^{-1})^*, w^{-1}$ denotes the word obtained by exchanging everywhere the letters x and x^{-1} and reversing the order of the letters. Now, for w, w' in $(X \cup X^{-1})^*$, we say that w' is obtained from w by *word reversing* with respect to f if one can transform w into w' by repeatedly replacing subwords of the form $x^{-1} \cdot y$ with the corresponding words $f(x, y) \cdot f(y,x)^{-1}$. It is easy [6] to prove that, starting with an arbitrary word w in $(X \cup X^{-1})^*$, word reversing leads to at most one word of the form $u \cdot v^{-1}$ with u, v positive, i.e., involving no letter in X^{-1}, and that such words are terminal with respect to word reversing. When they exist, the words u and v are called the (right) numerator and denominator of w, denoted by $N(w)$ and $D(w)$, respectively. We also define a (possibly partial) binary operation on X^* by $u\backslash v = N(u^{-1} \cdot v)$. Observe that $x\backslash y = f(x, y)$ holds for all x, y in X.

The compatibility between the braid complement and the LD complement extends to the operation $\backslash$ on words and to the numerators and denominators:

Lemma 3.2. (i) *Assume that u, v are positive words in $\boldsymbol{A}^*$ and $u\backslash v$ exists. Then we have*

$$pr(u\backslash v) = pr(u)\backslash pr(v). \tag{3.2}$$

(ii) *Assume that the word* w *of* $(\boldsymbol{A} \cup \boldsymbol{A}^{-1})^*$ *is reversible to the word* w'. *Then the braid word* $pr(w)$ *is reversible to the braid word* $pr(w')$. *In particular, we have*

$$pr(N(w)) = N(pr(w)) \quad \text{and} \quad pr(D(w)) = D(pr(w)) \tag{3.3}$$

whenever $N(w)$ *and* $D(w)$ *exist.*

Proof. Use an induction on the number of reversing steps. □

The previous result will allow us to reprove all properties of the braid complement, and, therefore, a number of classical properties of the braid monoid B_∞^+, from the corresponding properties of the LD complement.

Definition. Assume that f is a complement on X. We say that f is *atomic* if there exists a mapping v of X^* into $\boldsymbol{N}$ such that $v(x) > 0$ holds for every x in X, $v(xu) > v(u)$ holds for every x in X and every u in X^*, and $v(uxf(y,x)v) = v(u, yf(x,y)v)$ holds for all u, v in X^* and all x, y in X.

Lemma 3.3. (i) *The braid complement is atomic.*
(ii) *The LD complement is atomic.*

Proof. In the case of braids, the length mapping satisfies all requirements trivially. In the case of the LD complement, some LD-relations do not preserve the length of the words, and the argument is more delicate. Assume that u is a positive word in $\boldsymbol{A}^*$. By Proposition 1.3, there exists a unique pair of LD-equivalent canonical terms $(t_u^{\mathrm{L}}, t_u^{\mathrm{R}})$, such that LD_u maps the term t to the term t' if and only if there exists a substitution h such that t is $(t_u^{\mathrm{L}})^h$ and t' is $(t_u^{\mathrm{R}})^h$. Let us define

$$v(u) = size(t_u^{\mathrm{R}}) - size(t_u^{\mathrm{L}}), \tag{3.4}$$

where, for t a term, size(t) is the number of occurrences of variables in t. By construction, v takes values in $\boldsymbol{N}$, and $v(\alpha) = 1$ holds for every address α for expanding t_α^{L} to t_α^{R} consists in doubling the variable occurring at $\alpha 0$ in t_α^{L}. If $u' \equiv^+ u$ holds, we have $LD_u = LD_{u'}$, hence $t_u^{\mathrm{L}} = t_{u'}^{\mathrm{L}}$ and $t_u^{\mathrm{R}} = t_{u'}^{\mathrm{R}}$, and, finally, $v(u') = v(u)$. Assume now $\alpha \in \boldsymbol{A}$ and $u \in \boldsymbol{A}^*$. By definition, we have $t_{\alpha\cdot u}^{\mathrm{R}} = ((t_{\alpha\cdot u}^{\mathrm{L}})\alpha)u$, hence there exists a substitution h satisfying $(t_{\alpha\cdot u}^{\mathrm{L}})\alpha = (t_u^{\mathrm{L}})^h$ and $t_{\alpha\cdot u}^{\mathrm{R}} = (t_u^{\mathrm{R}})^h$. We deduce

$$\begin{aligned}
v(\alpha\cdot u) &= \mathrm{size}(t_{\alpha\cdot u}^{\mathrm{R}}) - \mathrm{size}(t_{\alpha\cdot u}^{\mathrm{L}})\\
&= \mathrm{size}(t_{\alpha\cdot u}^{\mathrm{R}}) - \mathrm{size}((t_{\alpha\cdot u}^{\mathrm{R}})\alpha) + \mathrm{size}((t_{\alpha\cdot u}^{\mathrm{R}})\alpha) - \mathrm{size}(t_{\alpha\cdot u}^{\mathrm{L}})\\
&= \mathrm{size}((t_u^{\mathrm{R}})^h) - \mathrm{size}((t_u^{\mathrm{L}})^h) + \mathrm{size}((t_{\alpha\cdot u}^{\mathrm{L}})\alpha) - \mathrm{size}(t_{\alpha\cdot u}^{\mathrm{L}})\\
&> \mathrm{size}((t_u^{\mathrm{R}})^h) - \mathrm{size}((t_u^{\mathrm{L}})^h) \geq \mathrm{size}(t_u^{\mathrm{R}}) - \mathrm{size}(t_u^{\mathrm{L}}) = v(u).
\end{aligned}$$

Hence the mapping v satisfies the requirements. □

Definition. Assume that f is a complement on X. We say that f is *coherent* (*on the right*) if, for every triple (x,y,z) in X^3, we have

$$((x\backslash y)\backslash(x\backslash z))\backslash((y\backslash x)\backslash(y\backslash z)) = \varepsilon.$$

Lemma 3.4. (i) *The braid complement is coherent.*
(ii) *The LD complement is coherent.*

Proof. For (i), the verification is essentially Garside's Theorem H of [12]. For (ii), we refer to [5]. □

It is proved in [6] that: If f is a complement on X that is atomic and coherent, then the monoid $\langle X; \{xf(y,x) = yf(x,y); x,y \in X\}\rangle$ is left cancellative, and any two elements a, b of this monoid that admit a common right multiple admit a right lcm; in this case, if the words u, v represent a and b, then $u(u\backslash v)$ exists and it represents the right lcm of a and b. Applying this to the current framework, and owing to the fact that right common multiples exist in M_{LD} by Proposition 2.18, we deduce the following results:

Proposition 3.5. (i) *The monoid M_{LD} is left cancellative.*
(ii) *Every pair of elements of M_{LD} admits a right lcm, the operation $\backslash$ is defined everywhere on $\boldsymbol{A}^*$, and, if the positive words u, v represent the elements a and b of M_{LD}, respectively, then $u(u\backslash v)$ represents the right lcm of a and b.*

3.2. Simple elements

Let us define a simple braid in B_n to be a positive braid that is a left divisor of Garside's fundamental braid Δ_n. Simple braids play a significant role in the study of braids [12]. In this section, we develop the analogous notion of a simple element in the monoid M_{LD}.

By construction — or using the Coxeter presentation of the symmetric group — there exists a surjective projection of the braid group B_∞ onto the symmetric group S_∞ of all permutations of the positive integers that move only finitely many integers. We obtain a section for this projection by introducing, for every permutation f, a positive braid of minimal possible length that projects on f. Let us say that a braid is a permutation braid if it is the image of a permutation under the previous section. A significant result about braids is the fact that a braid is a permutation braid if and only if it is simple. This result leads in particular to the greedy normal form of [1,10,11].

We show now how to obtain a similar equivalence in the case of the monoid M_{LD}. This result involves the notions of a permutation-like element and of a simple element in M_{LD}, which extend the notion of a permutation braid and of a simple braid, respectively. The first notion will be defined using an explicit, syntactic method, while the second one involves the action of M_{LD} on terms via self-distributivity, and the equivalence result can be seen as a completeness theorem connecting a syntactic and a semantic notion.

We recall that, for $\alpha \in \boldsymbol{A}$ and $r \geq 0$, $\alpha^{(p)}$ is defined to be $\alpha 1^{r-1} \cdot \alpha 1^{r-2} \cdot \ldots \cdot \alpha 1 \cdot \alpha$ for $r \geq 1$, and to be ε for $p = 0$. For α, $\beta \in \boldsymbol{A}$, we define $\alpha \geq \beta$ to mean that α is a prefix of β, or α lies on the right of β, thus, for instance, $\phi \geq 1 \geq 0$ holds.

Definition. We say that the word u of $\boldsymbol{A}^*$ is a *permutation-like* word if u has the form $\alpha_1^{(r_1)} \ldots \alpha_\ell^{(r_\ell)}$ with $\alpha_1 \geq \cdots \geq \alpha_\ell$; in this case, for every address α, the *exponent* $\mathrm{e}(\alpha, u)$ of α in u is defined to be the integer r such that $\alpha^{(r)}$ appears in u, if it exists, and to be 0 otherwise. An element of M_{LD} is said to be a *permutation-like* element if it can be represented by a permutation-like word.

As $\alpha^{(0)}$ has been defined to be the empty word, a permutation-like word can be written as $\prod_{\alpha \in \boldsymbol{A}}^{\geq} \alpha^{(r_\alpha)}$, where $(r_\alpha; \alpha \in \boldsymbol{A})$ is a sequence of nonnegative integers with finitely many positive entries. Observe that a length 1 word, i.e., a single address, is a permutation-like word. It is easy to check that the projection of a permutation-like element of M_{LD} on B_∞^+ is a permutation braid.

Example 3.6. Let $w = 11 \cdot 1 \cdot \phi \cdot 1 \cdot 001 \cdot 00$. Then w is a permutation-like word, since we have $w = (11 \cdot 1 \cdot \phi) \cdot (1) \cdot (001 \cdot 00) = \phi^{(3)} \cdot 1^{(1)} \cdot 00^{(2)}$, and $\phi \geq 1 \geq 00$ holds. We have $\mathrm{e}(\phi, w) = 3$, $\mathrm{e}(0, w) = 0$, and $\mathrm{e}(1, w) = 1$.

By definition of the ordering on addresses, a permutation-like word always has the form $\phi^{(r)} \cdot 1u_1 \cdot 0u_0$, where u_1 and u_0 are permutation-like words. This will enable us to develop inductive arguments.

Lemma 3.7. *A permutation-like element in M_{LD} admits a unique representation by a permutation-like word. More precisely, if a is a permutation-like element, the unique permutation-like word that represents a depends on the operator LD_a only.*

Proof. Assume that u is a permutation-like word. We show that the exponents of u are determined by the operator LD_u using induction on the size of t_u^{L}. For $\mathrm{size}(t_u^{\mathrm{L}}) = 1$, we have $LD_u = id$, hence $u = \varepsilon$, and the result is true. Otherwise, assume $u = \phi^{(r)} \cdot 1u_1 \cdot 0u_0$. Since $(t_u^{\mathrm{L}})\phi^{(r)}$ exists, we have $\mathrm{ht}_{\mathrm{R}}(t_u^{\mathrm{L}}) \geq r + 1$. Let $t_0 \cdot t_1 = (t_u^{\mathrm{L}})\phi^{(r)}$, and be $x_{f(i)}$ be the rightmost variable of the 1^i0th subterm of t_u^{L}. By construction, the rightmost variable of t_0 is $x_{f(r)}$. Now we have $t_u^{\mathrm{R}} = (t_u^{\mathrm{L}})u = (t_0)u_0 \cdot (t_1)u_1$, we deduce that $x_{f(r)}$ is the rightmost variable of the 0-th subterm of t_u^{R}. This shows that t_u^{R} determines r, and, therefore, so does u. Then, for $e = 0$ and $e = 1$, t_e belongs to the domain of LD_{u_e}, it is an injective term, and we have $\mathrm{size}(t_e) < \mathrm{size}(t_u^{\mathrm{L}})$. As t_e is a substitute of $t_{u_e}^{\mathrm{L}}$, we deduce $\mathrm{size}(t_{u_e}^{\mathrm{L}}) < \mathrm{size}(t_u^{\mathrm{L}})$, hence, by induction hypothesis, $(t_e)u_e$ determines the exponents in u_e, and so does $(t)u$, since $(t_e)u_e$ is $\mathrm{sub}((t)u, e)$. $\square$

It follows that, for every permutation-like element a and every address α, we can define without ambiguity the exponent of α in a as the exponent of α in the unique permutation-like word that represents a.

We introduce now a second notion of simplicity for positive words by means of their action on injective terms.

Definition. If t is a term, the variable x_i is said to *cover* the variable x_j in t if there exist an address α in the skeleton of t such that x_i occurs in t at an address of the form $\alpha 1^p$, while x_j occurs in t at some address of the form $\alpha 0 \beta$. The term t is said to be *semi-injective* if no variable covers itself in t.

For a term t to be semi-injective means that, for every subterm s of t, the rightmost variable of s occurs only once in s. Thus, every injective term is semi-injective, but the converse is not true. For instance, the term $(x_1 \cdot x_2) \cdot (x_1 \cdot x_3)$, which is is not injective since x_1 occurs twice, is semi-injective.

Non-semi-injective terms have good closure properties. In the sequel, we write $var_{\mathrm{R}}(t)$ for the rightmost variable of t, i.e., for the unique variable that occurs in t at some address of the form 1^r.

Lemma 3.8. *Non-semi-injective terms are closed under substitution and LD-expansion.*

Proof. Assume that t is non-semi-injective. Then some variable x_i occurs both at $\alpha 1^r$ and $\alpha 0 \beta$ in t. Let h be an arbitrary substitution, and let $x_k = var_{\mathrm{R}}(h(x_i))$, $q = ht_{\mathrm{R}}(h(x_i))$. Then x_k occurs at $\alpha 1^{r+q}$ and $\alpha 0 \beta 1^q$ in t^h. Hence t^h is not semi-injective. On the other hand, LD-expansions never delete covering: if x_i covers x_j in t, it covers x_j in every LD-expansion of t: it suffices to establish the result for basic LD-expansions by considering the various possible cases. This applies in particular when x_i covers itself. □

We introduce now a semantical notion of simplicity that is analogous to the condition that any two strands cross at most once in a braid diagram.

Definition. An element a of M_{LD} is said to be *simple* if the operator LD_a maps at least one term to a semi-injective term. A word on $\boldsymbol{A}$ is said to be simple if its class in M_{LD} is simple.

Lemma 3.9. *Assume that a is an element of M_{LD}. Then, the following are equivalent*:
(i) *The element a is simple*;
(ii) *The term t_a^{R} is semi-injective*;
(iii) *The operator LD_a maps every injective term to a semi-injective term.*

Proof. The term t_a^{L} is injective, and the operator LD_a maps t_a^{L} to t_a^{R}, so (iii) implies (ii), and (ii) implies (i). Assume (i). Let t be a term in the domain of LD_a such that

$(t)a$ exists and is semi-injective. There exists a substitution h satisfying $t = (t_a^{\mathrm{L}})^h$ and $(t)a = (t_a^{\mathrm{R}})^h$. By Lemma 3.8 $(t_a^{\mathrm{R}})^h$ being semi-injective implies t_a^{R} being semi-injective as well, so (ii) holds. Assume now (ii), and let t be an injective term in the domain of LD_a. Then, there exists a substitution h satisfying $t = (t_a^{\mathrm{L}})^h$, and t being injective means that we can assume that the image of every variable under h is an injective term, and the images of distinct variables involve distinct variables. Now we have $(t)a = (t_a^{\mathrm{R}})^h$, and such a term being not semi-injective would imply t_a^{R} itself being not semi-injective. □

Using the closure properties of non semi-injective terms, we obtain the following closure property for simple elements of M_{LD}. Observe that the corresponding result for permutation-like elements is not clear — a situation parallel to the case of simple braids and permutation braids.

Lemma 3.10. *Every divisor of a simple element of M_{LD} is simple.*

Proof. Assume that a is not simple, and let b, c be arbitrary elements of M_{LD}. The term t_{ba}^{R} is a substitute of t_a^{R}, and the term t_{bac}^{R} is an LD-expansion of the previous term. By hypothesis, t_a^{R} is not semi-injective, hence, by Lemma 3.8, t_{ba}^{R} and t_{bac}^{R} are not semi-injective either. Hence bac is not simple. □

We shall prove eventually that permutation-like elements and simple elements in M_{LD} coincide. For the moment, we observe that one direction is easy.

Lemma 3.11. *Every permutation-like element of M_{LD} is simple.*

Proof. Assume that a is a permutation-like element. We show that a is simple using induction on the size of t_a^{L}. By construction, a can be expressed (in a unique way) as $\phi^{(r)} \cdot sh_1(a_1) \cdot sh_0(a_0)$ where a_0 and a_1 are permutation-like elements. Let $t = t_a^{\mathrm{L}}$. Then $(t)\phi^{(r)}$ exists, and, therefore, we have $\mathrm{ht}_{\mathrm{R}}(t) \geq r+1$, i.e., we can write $t = t_0 \cdot \ldots \cdot t_{r+1}$. We find $(t)\phi^{(r)} = t'_0 \cdot t'_1$, with

$$t'_0 = t_0 \cdot \ldots \cdot t_{r-1} \cdot t_r, \quad t'_1 = t_0 \cdot \ldots \cdot t_{r-1} \cdot t_{r+1}.$$

By hypothesis, for $e = 1, 0$, t'_e is an injective term that lies in the domain of the operator LD_{a_e}, and we have $\mathrm{size}(t'_e) < \mathrm{size}(t)$, hence $\mathrm{size}(t_{a_e}^{\mathrm{L}}) < \mathrm{size}(t_a^{\mathrm{L}})$. By induction hypothesis, the LD-expansions $(t'_1)a_1$ and $(t'_0)a_0$ are semi-injective terms. Hence $(t)a$, which is $(t'_0)a_0 \cdot (t'_1)a_1$, is semi-injective as well, for the rightmost variable of $(t'_1)a_1$, which is $var_{\mathrm{R}}(t'_1)$, occurs neither in t'_0 nor in $(t'_0)a_0$. □

Example 3.12. We obtain in this way a criterion for proving that a given element of M_{LD} is *not* a permutation-like element. For instance, the element $g_\phi^+ \cdot g_\phi^+$ is not simple, and, therefore, it is not a permutation-like element. Indeed $(x_1 \cdot x_2 \cdot x_3)\phi \cdot \phi$ is the term $((x_1 \cdot x_2) \cdot x_1) \cdot ((x_1 \cdot x_2) \cdot x_3))$, which is not semi-injective, since the variable x_1 occurs both at 01 and 000.

Our goal is now to establish the converse of Lemma 3.11. We begin with a series of computational formulas. The point is to determine the permutation-like decomposition of the product $\alpha^{(p)} \cdot \phi^{(q)}$, when it exists. We separate two cases, according to whether α contains at least one 0 or not.

Lemma 3.13. *Assume $\alpha = 1^m 0\beta$. Then $\alpha^{(p)} \cdot \phi^{(q)}$ is simple for all p, q, and we have*

$$\alpha^{(p)} \cdot \phi^{(q)} \equiv^+ \begin{cases} \phi^{(q)} \cdot \alpha^{(p)} & \text{for } q < m, \\ \phi^{(q)} \cdot (01^m\beta)^{(p)} & \text{for } q = m, \\ \phi^{(q)} \cdot (1\alpha)^{(p)} \cdot (0\alpha)^{(p)} & \text{for } q > m. \end{cases}$$

Proof. Assume $p = 1$. For $m \geq q+1$, $1^m 0\beta$ commutes with every factor of the word $\phi^{(q)}$ by type 11 relations, so α commutes with $\phi^{(q)}$. For $m = q$, using q successive type 10 relations, we obtain

$$\begin{aligned} \alpha \cdot \phi^{(m)} = 1^m 0\beta \cdot 1^{m-1} \cdot \ldots \cdot \phi &\equiv^+ 1^{m-1} \cdot 1^{m-1}01\beta \cdot 1^{m-2} \cdot \ldots \cdot \phi \\ &\vdots \\ &\equiv^+ 1^{m-1} \cdot \ldots \cdot 1 \cdot 101^{m-1}\beta \cdot \phi \\ &\equiv^+ 1^{m-1} \cdot \ldots \cdot 1 \cdot \phi \cdot 01^m\beta = \phi^{(m)} \cdot 01^m\beta. \end{aligned}$$

For $m < q$, we find

$$\begin{aligned} \alpha \cdot \phi^{(q)} &= 1^m 0\beta \cdot (1^{m+1})^{(q-m-1)} \cdot 1^m \cdot \phi^{(m)} \\ &\equiv^+ (1^{m+1})^{(q-m-1)} \cdot 1^m 0\beta \cdot 1^m \cdot \phi^{(m)} && \text{(type } \perp) \\ &\equiv^+ (1^{m+1})^{(q-m-1)} \cdot 1^m \cdot 1^m 10\beta \cdot 1^m 00\beta \cdot \phi^{(m)} && \text{(type 0)} \\ &\equiv^+ (1^{m+1})^{(q-m-1)} \cdot 1^m \cdot 1^m 10\beta \cdot \phi^{(m)} \cdot 01^m 0\beta \\ &\equiv^+ (1^{m+1})^{(q-m-1)} \cdot 1^m \cdot \phi^{(m)} \cdot 1^m 10\beta \cdot 01^m 0\beta = \phi^{(q)} \cdot 1\alpha \cdot 0\alpha. && \text{(type 11)} \end{aligned}$$

Extending the result to the case $p > 1$ is easy in the first two cases. In the last case, we observe that $1\alpha 1^{p-1} \cdot 0\alpha 1^{p-1} \cdot \ldots \cdot 1\alpha \cdot 0\alpha$ is equivalent to $(1\alpha)^{(p)} \cdot (0\alpha)^{(p)}$ using type $\perp$ relations. $\square$

Lemma 3.14. *Assume $\alpha = 1^m$. Then $\alpha^{(p)} \cdot \phi^{(q)}$ is simple if and only if $m < q \leqslant m + p$ does not hold*; *in this case*, *we have*

$$\alpha^{(p)} \cdot \phi^{(q)} \equiv^+ \begin{cases} \phi^{(q)} \cdot \alpha^{(p)} & \text{for } q < m, \\ \phi^{(p+q)} & \text{for } q = m, \\ \phi^{(q)} \cdot (1^{m+1})^{(p)} \cdot (01^m)^{(p)} & \text{for } q > m + p. \end{cases}$$

Proof. For $q < m$, every factor in the word $\phi^{(q)}$ commutes with every factor in the word $\alpha^{(p)}$ by type 11 relations, so $\alpha^{(p)}$ and $\phi^{(q)}$ commute. For $q = m$, we have $\alpha^{(p)}\phi^{(q)} =$

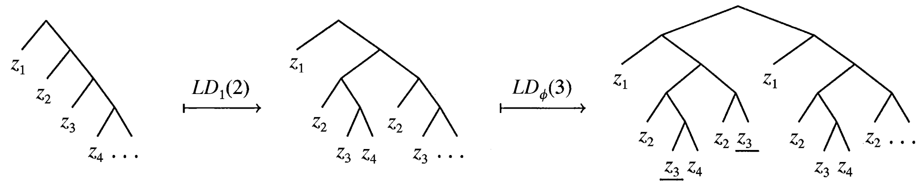


Fig. 2. A non-simple case: $m = 1$, $p = 2$, $q = 3$.

$\phi^{(p+q)}$. Assume $q > m+p$; we use induction on p. Assume first $p=1$, hence $q \geq m+2$. We have

$$\begin{aligned} 1^m \cdot \phi^{(q)} &= 1^m \cdot (1^{m+2})^{(q-m-2)} \cdot 1^{m+1} \cdot 1^m \cdot \phi^{(m)} \\ &\equiv^+ (1^{m+2})^{(q-m-2)} \cdot 1^m \cdot 1^{m+1} \cdot 1^m \cdot \phi^{(m)} && \text{(type 11)} \\ &\equiv^+ (1^{m+2})^{(q-m-2)} \cdot 1^{m+1} \cdot 1^m \cdot 1^{m+1} \cdot 1^m0 \cdot \phi^{(m)} && \text{(type 1)} \\ &= (1^m)^{(q-m)} \cdot 1^{m+1} \cdot 1^m0 \cdot \phi^{(m)} \\ &\equiv^+ (1^m)^{(q-m)} \cdot 1^{m+1} \cdot \phi^{(m)} \cdot 01^m && \text{(Lemma 3.13)} \\ &\equiv^+ (1^m)^{(q-m)} \cdot \phi^{(m)} \cdot 1^{m+1} \cdot 01^m = \phi^{(q)} \cdot 1^{m+1} \cdot 01^m && \text{(type 11).} \end{aligned}$$

Assume now $p > 1$. We have

$$\begin{aligned} (1^m)^{(p)} \cdot \phi^{(q)} &= (1^{m+1})^{(p-1)} \cdot 1^m \cdot \phi^{(q)} \\ &\equiv^+ (1^{m+1})^{(p-1)} \cdot \phi^{(q)} \cdot 1^{m+1} \cdot 01^m && \text{(ind. hyp.)} \\ &\equiv^+ \phi^{(q)} \cdot (1^{m+2})^{(p-1)} \cdot (01^{m+1})^{(p-1)} \cdot 1^{m+1} \cdot 01^m && \text{(ind. hyp.)} \\ &\equiv^+ \phi^{(q)} \cdot (1^{m+2})^{(p-1)} \cdot 1^{m+1} \cdot (01^{m+1})^{(p-1)} \cdot 01^m && \text{(type } \perp\text{)} \\ &= \phi^{(q)} \cdot (1^{m+1})^{(p)} \cdot (01^m)^{(p)}. \end{aligned}$$

The above explicit formulas show that, in the three previous cases, $\alpha^{(p)} \cdot \phi^{(q)}$ is a permutation-like element. So it only remains to prove that the product is not simple in the case $m < q \leq m+p$. By Lemma 3.11, it suffices to exhibit an injective term whose image under the operator $LD_{\alpha^{(p)} \cdot \phi^{(q)}}$ is not semi-injective. Let $t = x_1 \cdot \ldots \cdot x_{m+p+2}$. We find

$$(t)\alpha^{(p)} = x_1 \cdot \ldots \cdot x_m \cdot (x_{m+1} \cdot \ldots \cdot x_{m+p} \cdot x_{m+p+1}) \cdot x_{m+1} \cdot \ldots \cdot x_{m+p} \cdot x_{m+p+2}.$$

Applying the operator $LD_{\phi^{(q)}}$ to this term gives a term whose 01^m-subterm is

$$(x_{m+1} \cdot \ldots \cdot x_{m+p+1}) \cdot x_{m+1} \cdot \ldots \cdot x_{q+1},$$

and the rightmost variable of this subterm, namely x_{q+1}, also occurs in its left subterm, so it is not semi-injective — see an example, in Fig. 2. □

We can now determine whether a permutation-like element remains a permutation-like element when an additional factor $\phi^{(q)}$ is appended.

Lemma 3.15. *Assume that a is a permutation-like element in M_{LD}, and q is nonnegative. Let $r = q + \mathrm{e}(1^q, a)$. Then $a \cdot \phi^{(q)}$ is simple if $m + \mathrm{e}(1^m, a) < r$ holds for $0 \le m < q$; in this case, $a \cdot \phi^{(q)}$ is a permutation-like element, and we have $r = \mathrm{e}(\phi, a \cdot \phi^{(q)})$.*

Proof. In order to simplify notations, for $\gamma \in \boldsymbol{A}$, and $a \in M_{LD}$, we write γa for $sh_\gamma(a)$. Write

$$a = \prod_{m=0}^{\infty} (1^m)^{(r_m)} \cdot \prod_{m=\infty}^{0} 1^m 0 a_m,$$

where all a_m are permutation-like elements. We add the factor $\phi^{(q)}$ on the right, and try to push this factor to the left and integrate it in the decomposition. By Lemma 3.13, we cross the right product: $a \cdot \phi^{(q)}$ is equal to

$$\prod_{m=0}^{\infty} (1^m)^{(r_m)} \cdot \phi^{(q)} \cdot \prod_{m=\infty}^{q+1} 1^m 0 a_m \cdot 01^q a_q \cdot \prod_{m=q-1}^{0} (1^{m+1} 0 a_m \cdot 01^m 0 a_m),$$

hence, using type $\perp$ relations, to

$$\prod_{m=0}^{\infty} (1^m)^{(r_m)} \cdot \phi^{(q)} \cdot \prod_{m=\infty}^{q+1} 1^m 0 a_m \cdot \prod_{m=q-1}^{0} 1^{m+1} 0 a_m \cdot 01^q a_q \cdot \prod_{m=q-1}^{0} 01^m 0 a_m.$$

It remains to study the expression $\prod_{m=0}^{\infty} (1^m)^{(r_m)} \cdot \phi^{(q)}$. We use now Lemma 3.14 to push $\phi^{(q)}$ to the left. First, we have

$$\prod_{m=q}^{\infty} (1^m)^{(r_m)} \cdot \phi^{(q)} \equiv^+ \phi^{(r)} \cdot \prod_{m=q+1}^{\infty} (1^m)^{(r_m)},$$

with $r = q + r_q$, i.e., $r = q + \mathrm{e}(1^q, a)$, and we are left with $\prod_{m=0}^{q-1} (1^m)^{(r_m)} \cdot \phi^{(r)}$. By Lemma 3.14, two cases are possible. Either the condition $q - 1 + r_{q-1} \ge r$ holds, and then $(1^{q-1})^{(r_{q-1})} \phi^{(r)}$ is not simple, and, therefore, by Lemma 3.10, $w \cdot \phi^{(q)}$ is not either simple. Or $q - 1 + r_{q-1} < r$ holds, and $(1^{q-1})^{(r_{q-1})} \cdot \phi^{(r)}$ is a permutation element, and it is equal to $\phi^{(r)} \cdot (1^q)^{(r_{q-1})} \cdot (01^{q-1})^{(r_{q-1})}$. We can continue, and consider the product $(1^{q-2})^{(r_{q-2})} \cdot \phi^{(r)}$. Again two cases are possible: in the one case, $w \cdot \phi^{(q)}$ is not simple, in the other, it is a permutation-like element, we can push the factor $\phi^{(q)}$ to the left, and the process continues. Finally, if the condition $m + r_m < r$ fails for some m, $w \cdot \phi^{(q)}$ is not simple; if the condition holds for every m, the factor $\phi^{(q)}$ migrates to the leftmost position, and we obtain that $a \cdot \phi^{(p)}$ is equal to

$$\phi^{(r)} \cdot \prod_{m=0}^{q-1} (1^{m+1})^{(r_m)} \cdot \prod_{m=0}^{q-1} (01^m)^{(r_m)} \cdot \prod_{m=\infty}^{q+1} 1^m 0 a_m \cdot \prod_{m=q-1}^{0} 1^{m+1} 0 a_m \cdot 01^q a_q$$

$$\cdot \prod_{m=q-1}^{0} 01^m 0 a_m,$$

which can be rearranged using type $\perp$ relations and renumbering into

$$\phi^{(r)} \cdot \prod_{m=1}^{q} (1^m)^{(r_{m-1})} \cdot \prod_{m=\infty}^{q+1} 1^m 0 a_m \cdot \prod_{m=q}^{1} 1^m 0 a_{m-1} \cdot \prod_{m=0}^{q-1} (01^m)^{(r_m)} \cdot 01^q a_q \cdot \prod_{m=q-1}^{0} 01^m 0 a_m,$$

an explicit permutation-like element of M_{LD}. $\square$

Proposition 3.16. *An element of M_{LD} is permutation-like if it is simple.*

Proof. We have already seen that every permutation-like element is simple. We establish now that a being simple implies a being a permutation-like element using induction on size(t_a^{L}). For size$(t_a^{\mathrm{L}}) = 1$, we have $a = 1$, both a permutation-like element and a simple element. Assume now $a \neq 1$. Then a can be decomposed as $b \cdot \alpha^{(q)}$. By Lemma 3.10, b is simple, so, by induction hypothesis, it is a permutation-like element. We show inductively on the length of the address α that $b \cdot \alpha^{(q)}$ is a permutation-like element. For $\alpha = \phi$, the previous lemma gives the result. Otherwise, assume $\alpha = e\beta$, with $e = 0$ or $e = 1$. There exist an integer r and permutation-like elements a_1, a_0 such that a is equal to $\phi^{(r)} \cdot sh_1(a_1) \cdot sh_0(a_0)$. By Lemma 3.10 again, the element $sh_e(a_e) \cdot \alpha^{(q)}$ is simple, which implies that $a_e \cdot \beta^{(q)}$ is simple too, since a subterm of a semi-injective term is semi-injective. By induction hypothesis, $a_e \cdot \beta^{(q)}$ is simple, and so are $sh_e(a_e) \cdot \alpha^{(q)}$, and $\phi^{(r)} \cdot sh_{1-e}(a_{1-e}) \cdot sh_e(a_e) \cdot \alpha^{(q)}$. This completes the induction. $\square$

Remark. The braid counterpart of the previous result is the equivalence of simple braids and permutation braids, more precisely the fact that every simple braid in B_n is a left divisor of Δ_n. The key point in the latter fact is the exchange lemma for the symmetric group S_n, a special case of the well-known exchange lemma for Coxeter groups. The above argument can be seen as a tree version of the exchange lemma.

4. Applications

Once we know that simple elements and permutation-like elements coincide in the monoid M_{LD}, further results can be deduced easily.

4.1. Simple LD-expansions

What makes simple braids remarkable is the property that the right lcm of two simple braids in the monoid B_∞^+ is still a simple braid. In particular, the braid Δ_n is a maximal simple braid in B_n^+, and it is the right lcm of all such simple braids. Here we prove similar results in the case of the monoid M_{LD}, the role of the braids Δ_n being played by the elements Δ_t represented by the words $\boldsymbol{\Delta}_t$.

Definition. The term t' is a *simple* LD-expansion of the term t if there exists a simple word u such that LD_u maps t to t'.

By Lemma 3.7, there exists a one-to-one correspondence between the simple LD-expansions of a term t and the permutation-like elements a in M_{LD} such that t belongs to the domain of LD_a.

Proposition 4.1. *For every term t, the term ∂t is the maximal simple LD-expansion of t, and $\boldsymbol{\Delta}_t$ is the (unique) permutation-like word u such that LD_u maps t to ∂t.*

Proof. We already know that $LD_{\boldsymbol{\Delta}_t}$ maps t to ∂t. That $\boldsymbol{\Delta}_t$ is a permutation-like word follows from its explicit definition. So it remains to prove using induction on the size of t that no LD-expansion of ∂t is a semi-injective term. Assume $t = t_0 \cdot t_1$. We consider first LD-expansion at ϕ. The equality $\partial t = \partial t_0 * \partial t_1$ shows that every variable occurring in t except possibly the rightmost one occurs both in the left and the right subterm of ∂t. So the rightmost variable of $\mathrm{sub}(\partial t, 10)$, say x_i, occurs in $\mathrm{sub}(\partial t, 0)$ also, hence, when LD_ϕ is applied to ∂t, x_i covers itself in the resulting LD-expansion, which therefore is not semi-injective. Consider now LD-expansion at α, where α is a nonempty address, say $\alpha = e\beta$ with $e = 0$ or $e = 1$. By construction, we have $\mathrm{sub}((\partial t)\alpha, e) = (\partial t_e)\beta$, which, by induction hypothesis, is not a semi-injective term. So $(t)\alpha$ is not either semi-injective. □

Corollary 4.2. *For every term t, the class Δ_t of $\boldsymbol{\Delta}_t$ in M_{LD} is simple, and it is maximal in the sense that $\Delta_t a$ is simple for no element a such that the term $(t)\Delta_t \cdot a$ exists.*

Proposition 4.3. *For every a of M_{LD}, the following are equivalent:*
(i) *The element a is simple.*
(ii) *There exists a term t such that a is a left divisor of Δ_t in M_{LD}.*
(iii) *For every term t such that $(t)a$ exists, the element a is a left divisor of Δ_t in M_{LD}.*

Proof. By definition, (iii) implies (ii), and, by the previous corollary, (ii) implies (i). So the point is to prove that (i) implies (iii). We prove using induction on the size of t that, if u is a permutation-like word and $(t)u$ is defined, then there exists a word v satisfying $u \cdot v \equiv^+ \boldsymbol{\Delta}_t$. The result is obvious when t is a variable. Otherwise, let $r + 1 = ht_{\mathrm{R}}(t)$. By definition, the term t belongs to the domain of the operator LD_u, the inequality $m + \mathrm{e}(1^m, u) \le r$ holds for $0 \le m \le r$, so there exists a least q satisfying $q + \mathrm{e}(1^q, u) = r$. By Lemma 3.15, we deduce that $u \cdot \phi^{(q)}$ is simple, and that $\mathrm{e}(\phi, u \cdot \phi^{(q)}) = r$ holds, which means that there exist simple words u_1, u_0 satisfying

$$u \cdot \phi^{(q)} \equiv^+ \phi^{(r)} \cdot 1u_1 \cdot 0u_0.$$

By construction, $(t)\phi^{(r)}$ is defined. Let $s_0 \cdot s_1 = (t)\phi^{(r)}$. By definition, the term $(s_e)u_e$ is defined for $e = 1, 0$, and, by construction, we have $\mathrm{size}(s_e) < \mathrm{size}(t)$. Hence, by induction hypothesis, there exists a word v_e satisfying $u_e \cdot v_e \equiv^+ \varDelta_{s_e}$. We obtain

$$u \cdot \phi^{(q)} \cdot 1v_1 \cdot 0v_0 \equiv^+ \phi^{(r)} \cdot 1u_1 \cdot 0u_0 \cdot 1v_1 \cdot 0v_0 \equiv^+ \phi^{(r)} \cdot 1\varDelta_{s_1} \cdot 0\varDelta_{s_0} = \varDelta_t. \qquad \square$$

Proposition 4.4. *Any two simple elements of M_{LD} admit a simple right lcm.*

Proof. Assume that a, b are simple elements of M_{LD}. Let t be a term both in the domain of LD_a and in domain of LD_b. Then $\varDelta_t$ is a common right multiple of a and b, hence it is a right multiple of the right lcm of a and b. Hence the latter element, which divides an element of the form $\varDelta_t$, is simple. $\square$

As every (left or right) divisor of a simple element of M_{LD} is still a simple element, we deduce from Proposition 4.4 that, if a and b are simple, so is the (unique) element $a\backslash b$ such that $a(a\backslash b)$ is the right lcm of a and b.

4.2. Normal form

We construct now a unique normal from for the elements of M_{LD}. It is an exact counterpart to the right greedy normal form for the braid monoids [1,10,11] — on which it projects.

Definition. Assume that a, b are simple elements of M_{LD}. We say that a is *orthogonal* to b if, for each address α such that g_α^+ is a left divisor of b, $a \cdot g_\alpha^+$ is not simple.

Proposition 4.5. *Every element of M_{LD} admits a unique decomposition of the form $a_1 \cdot \ldots \cdot a_p$, where $a_1, \ldots, a_p$ are simple and, for every $k \geq 2$, a_{k-1} is orthogonal to a_k.*

Proof. Let a be an arbitrary element of M_{LD}. We prove the existence of an expression of a satisfying the above conditions using induction on $v(a)$, defined as the common value of $v(u)$ for u a word on $\boldsymbol{A}$ representing a. For $v(a) = 0$, we have $a = 1$, and the result is obvious. Assume $a \neq 1$. For a' a simple left divisor of a, we have $v(a') \leq v(a)$ by construction, so there exists at least one simple left divisor a_1 of a such that $v(a_1)$ has the maximal possible value. As a is not 1, there exists at least one address α such that g_α^+ is a left divisor of a, and, as g_α^+ is simple, we deduce that a_1 cannot be 1. Write $a = a_1 \cdot b$. Then we have $v(a) > v(b)$. By induction hypothesis, b admits a decomposition $b = a_2 \cdot \ldots \cdot a_p$ that satisfies the conditions of the propostion. We deduce $a = a_1 \cdot a_2 \cdot \ldots \cdot a_p$, and it remains to prove that a_1 is orthogonal to a_2. Assume that g_α^+ is a nontrivial left divisor of a_2 in M_{LD}. Then g_α^+ is a left divisor of b, and $a_1 \cdot g_\alpha^+$ is a left divisor of a. This implies that $a_1 \cdot g_\alpha^+$ is not simple, for, otherwise, the condition $v(a_1 \cdot g_\alpha^+) > v(a_1)$ would contradict the definition of a_1.

For uniqueness, it suffices to prove that, if $(a_1, \ldots, a_p)$ is a sequence of simple elements of M_{LD} such that, for $k \geq 2$, a_{k-1} is orthogonal to a_k, then a_1 is determined by the product $a_1 \dots a_p$. Indeed, M_{LD} is left cancellative, and an induction then shows that $a_2, \dots, a_p$ are determined as well. So, assume $a = a_1 \cdot \dots \cdot a_p$, with $(a_1, \dots, a_p)$ as above. By construction, a_1 is a simple left divisor of a. Assume that c_1 is a nontrivial element of M_{LD} such that $a_1 \cdot c_1$ is simple. Define inductively $c_k = a_k \backslash c_{k-1}$ for $2 \leq k \leq p$. The hypothesis that $a_1 \cdot c_1$ is simple implies that c_1 is simple. Then, $a_2 \cdot c_2$ is the right lcm of a_2 and c_1, hence it is simple as well, and this in turn implies that c_2 is simple. Similarly, we show using induction on k that $a_k \cdot c_k$ and c_k are simple for every k. Now, the hypotheses that c_1 is not 1 and that a_2 is orthogonal to a_1 imply that c_1 is not a left divisor of a_2, and, therefore, we have $c_2 \neq 1$. Repeating the argument yields $c_k \neq 1$ for every k. In particular, we have $c_p \neq 1$. Now, by construction, we have $c_p = (a_2 \cdot \dots \cdot a_p) \backslash c_1$, and $c_p \neq 1$ means that c_1 is not a left divisor of $a_2 \cdot \dots \cdot a_p$, hence that $a_1 \cdot c_1$ is not a left divisor of a. Thus we have proved that a_1 is a simple left divisor of a with maximal value of v. It remains to observe that such an element is unique. Now, assume that a_1, a_1' are such elements. Then the right lcm of a_1 and a_1' is still a left divisor of a, it is simple by Proposition 4.4, and the assumption $v(a_1) = v(a_1') = v(a_1(a_1 \backslash a_1'))$ implies $a_1' = a_1$. □

4.3. The Embedding Conjecture

In [12], Garside proves that the braid monoid B_∞^+ embeds in the braid group B_∞^+, which implies that B_∞ is the group of fractions of B_∞^+. Here we briefly discuss the similar question for the monoid M_{LD} and the group G_{LD}.

Conjecture 4.6. *The monoid M_{LD} embeds in the group G_{LD}, i.e., for all words u, u' on $\boldsymbol{A}$, $u' \equiv u$ implies (and, therefore, is equivalent to) $u' \equiv^+ u$.*

Several equivalent forms can be stated.

Proposition 4.7. *Conjecture* 4.6 *is equivalent to each of the following statements*:
(i) *The monoid M_{LD} admits right cancellation.*
(ii) *The monoid $\mathscr{G}_{LD}^+$ is isomorphic to the monoid M_{LD}, i.e., for all words u, u' in $\boldsymbol{A}^*$, $LD_{u'} = LD_u$ implies (and, therefore, is equivalent to) $u' \equiv^+ u$.*

Proof. The equivalence with (i) follows from the results of [6], as we know that M_{LD} is associated with an atomic, coherent, and convergent complement (the latter meaning that word reversing always terminates, which is a consequence of the existence of common right multiples). The equivalence with (ii) follows from Proposition 1.5, which tell us that $LD_{u'} = LD_u$ is equivalent to $u' \equiv u$. □

Definition. Assume that a is an element of M_{LD}. We say that the Embedding Conjecture is true *for a* if the canonical projection of M_{LD} onto G_{LD}^+ is injective on a, i.e., if $LD_a \neq LD_{a'}$ holds for every $a' \neq a$ in M_{LD}.

Thus, Conjecture 4.6 is true if the Embedding Conjecture is true for every element of M_{LD}.

Proposition 4.8. *The Embedding Conjecture is true for every simple element of M_{LD}.*

Proof. Assume that a is a simple element of M_{LD}, and the operators LD_a and $LD_{a'}$ coincide. Hence, by definition, a' is simple as well, and, by Lemma 3.7, both a and a' are represented by permutation-like word determined by the operator LD_a. $\square$

No proof of the Embedding Conjecture is known to date. Let us mention that further partial results can be established using completely different methods. In particular, it is proved in [7] that the Embedding Conjecture is true for every element of M_{LD} that is a right divisor of some element $\Delta_t^{(k)}$, as well as for every element of the submonoid of M_{LD} generated by the elements $g_{1^i}^{+}$.

References

[1] S.I. Adjan, Fragments of the word Delta in a braid group, Mat. Zam. Acad. Sci. SSSR 36(1) (1984) 25–34 (translated Math. Notes of the Acad. Sci. USSR 36(1) (1984) 505–510).

[2] P. Dehornoy, Free distributive groupoids, J. Pure Appl. Algebra 61 (1989) 123–146.

[3] P. Dehornoy, Structural monoids associated to equational varieties, Proc. Amer. Math. Soc. 117 (2) (1993) 293–304.

[4] P. Dehornoy, Braid groups and left distributive operations, Trans. Amer. Math. Soc. 345 (1) (1994) 115–151.

[5] P. Dehornoy, The structure group for the associativity identity, J. Pure Appl. Algebra 111 (1996) 59–82.

[6] P. Dehornoy, Groups with a complemented presentation, J. Pure Appl. Algebra 116 (1997) 115–137.

[7] P. Dehornoy, The fine structure of LD-equivalence Advances in Math, to appear.

[8] P. Dehornoy, L. Paris, Garside groups, a generalization of Artin groups, Proc. London Math. Soc. 79 (3) (1999) 569–604.

[9] P. Deligne, Les immeubles des groupes de tresses généralisés, Invent. Math. 17 (1972) 273–302.

[10] E.A. Elrifai, H.R. Morton, Algorithms for positive braids, Quart. J. Math. Oxford 45 (2) (1994) 479–497.

[11] D. Epstein et al., Word Processing in Groups, Jones & Barlett, Boston, MA, 1992.

[12] F.A. Garside, The braid group and other groups, Quart. J. Math. Oxford 20 (78) (1969) 235–254.

[13] E. Ghys, V. Sergiescu, Sur un groupe remarquable de diffomorphismes du cercle, Comment. Math. Helverici 62 (1987) 185–239.

[14] R. Laver, The left distributive law and the freeness of an algebra of elementary embeddings, Adv. Math. 91 (2) (1992) 209–231.

[15] R. Laver, On the algebra of elementary embeddings of a rank into itself, Adv. Math. 110 (1995) 334–346.

[16] R. McKenzie, R.J. Thompson, An elementary construction of unsolvable word problems in group theory, in: Z. Boone et al. (Eds.), Word Problems, Studies in Logic, Vol. 71, North-Holland, Amsterdam, 1973.

[17] K. Tatsuoka, An isoperimetric inequality for Artin groups of finite type, Trans. Amer. Math. Soc. 339 (2) (1993) 537–551.